AMERICAN
JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

VOLUME LXXIX

1957

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

AMERICAN
JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

Volume LXXIX, Number 1
JANUARY, 1957

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

CONTENTS

The AMERICAN JOURNAL OF MATHEMATICS appears four times yearly.

The subscription price of the JOURNAL is $8.50 in the U. S.; $8.75 in Canada; and $9.00 in other foreign countries. The price of single numbers is $2.50.

Manuscipts intended for publication in the JOURNAL should be sent to Professor AUREL WINTNER, The Johns Hopkins University, Baltimore 18, Md.

Subscriptions to the JOURNAL and all business communications should be sent to THE JOHNS HOPKINS PRESS, BALTIMORE 18, MARYLAND, U. S. A.

THE JOHNS HOPKINS PRESS supplies to the authors 100 free reprints of every article appearing in the AMERICAN JOURNAL OF MATHEMATICS. On the other hand, neither THE JOHNS HOPKINS PRESS nor the AMERICAN JOURNAL OF MATHEMATICS can accept orders for additional reprints. Authors interested in securing more than 100 reprints are advised to make arrangements directly with the printers, J. H. FURST Co., 20 HOPKINS PLACE, BALTIMORE 1, MARYLAND.

The typescripts submitted can be in English, French, German or Italian and should be prepared in accordance with the instructions listed on the inside back cover of this issue.

Entered as second-class matter at the Baltimore, Maryland, Postoffice, acceptance for mailing at special rate of postage provided for in Section 1103, Act of October 3, 1917, Authorized on July 3, 1918.

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

suffi
diffe
roug

gen
ana
mar
of t
are
syst
inte
fold
equ
exar
p a
on a
If I
are
$(x,$
the
equ
inte

Fix
rest
line
ind
selv

1585

8841A

new

ON E. CARTAN'S PROLONGATION THEOREM OF EXTERIOR DIFFERENTIAL SYSTEMS.*

By Masatake Kuranishi.

Introduction. The purpose of the present paper is to give necessary and sufficient conditions for E. Cartan's conjecture on the prolongations of exterior differential system ([1], p. 116) to be true. To begin with, we shall explain roughly what the problem is.

An exterior differential system is defined to be a finite set of homogeneous analytic differential forms on a domain D in a real euclidean space; analytic functions are considered as differential forms of degree 0. A submanifold D_1 of D is called an integral manifold (or integral, or solution), of the system if the differential forms on D_1 induced by those in the system are always zero forms. The main purpose of the theory of exterior differential systems is, it seems to the writer, to find an effective method to construct all integral manifolds and to clarify the structure of the set of all integral manifolds. The theory is essentially a theory of systems of partial differential equations. Namely, given a system of partial differential equations, for example $F_\alpha(x, y, z, \partial z/\partial x, \partial z/\partial y) = 0$, we construct, introducing new variables p and q, a differential system consisting of $F_\alpha(x, y, z, p, q)$, $dz - pdx - qdy$ on an appropriate domain in the five dimensional euclidean space (x, y, z, p, q). If D_1 is a two dimensional integral manifold of this system and if dx and dy are linearly independent on D_1, we can express the submanifold in the form $(x, y, z(x, y), p(x, y), q(x, y))$. Then the function $z(x, y)$ is a solution of the original equations. Conversely if $z(x, y)$ is a solution of the original equations, the submanifold $(x, y, z(x, y), [\partial z/\partial x](x, y), [\partial z/\partial y](x, y))$ is an integral manifold of the system.

The above observation suggests the following restriction to the problem. Fix a set of linearly independent Pfaffian forms $dx^1, \cdots, dx^p$ on D and restrict our attention to the integral manifolds on which $dx^1, \cdots, dx^p$ are linearly independent. In this case, the functions $x^1, \cdots, x^p$ will be called independent variables. In the present paper, we shall mainly concern ourselves with this restricted problem.

The problem, which is to find a general method to construct all integral

* Received January 26, 1956.

manifolds, seems rather hard. Consequently, the results obtained so far are limited to furnish methods to construct integral manifolds satisfying some regularity conditions. For example, E. Cartan introduced the notion of general solutions of exterior differential systems and found a method to construct all general solutions. But unfortunately, there exist even examples of exterior differential systems which have integral manifolds but all the integral manifolds of the systems are not general solutions (cf. Example 1). Cartan's idea to proceed further starting from the theory of general solutions was to construct canonically new differential systems on new domains in such a way that the integral manifolds of the original systems correspond naturally in one-to-one manner to the integral manifolds of the newly constructed systems. If one constructs the new systems appropriately, it may possibly happen that an integral manifold of the original system which is not a general solution corresponds to a general solution of a newly constructed one.

For this purpose, E. Cartan defined the notion of prolongations of exterior differential systems, which is essentially to add partial derivatives of the unknown functions to the original systems of partial differential equations, and he said that, under certain conditions which are not easy to state precisely ([1], p. 116), every integral manifold will become a general solution after a finite number of prolongations. In the present paper, we shall justify this conjecture, giving a necessary and sufficient condition (cf. *Fundamental theorem*, § 6, Chapter III). Though E. Cartan considered two kinds of prolongations, that is, total and partial, we shall consider here only total prolongations. We shall also neglect the process of adding functions to the given system.

Since the theory developed so far is purely local, we shall restrict ourselves to differential systems on domains in real euclidean spaces. But it is easy to describe the theory on arbitrary real analytic manifolds, using the language in the theory of sheaves.

After some preliminaries, we shall summarize, in Chapter I, the Cartan-Kähler theory of exterior differential systems; except in a few cases the proofs are omitted. In Chapter II, we shall introduce the notion of normal exterior differential systems, and their prolongations will be examined. In Chapter III, after some preliminary notions are introduced and studied, the fundamental theorem will be formulated and proved.

Let me explain the expression "mod A," where A is a subspace of a vector space B. The writer uses this expression in two different meanings. By the first usage, it indicates the image in the factor space B/A by the

natural mapping. For instance, $(b \bmod A)$, where b is an element of B, means the image of b in the factor space B/A by the natural mapping, and if he says "$b_1, \cdots, b_n$ are linearly independent $\bmod A$," he means that $(b_1 \bmod A), \cdots, (b_l \bmod A)$ are linearly independent. The second usage occurs when B is a subspace in a ring. For instance, "$b_1 \equiv b_2 \pmod A$" means that $b_1 - b_2$ is in the ideal generated by A. The meaning will always, we hope, be clear from the context.

The writer owes thanks to Professor S. Chern for a valuable suggestion on the theory of exterior differential systems, and to Professor T. Nakayama for useful suggestions on the algebraic tools in this paper. The writer was introduced to the theory of exterior differential systems in the seminar by Professor Y. Matsushima at Nagoya University, 1952-53 and the formulation of the theory in §§ 1-3 of Chapter I is mainly borrowed from his seminar. The writer wishes to express his grateful thanks to all of them.

1. Preliminaries. As for the fundamental concepts in the theory of manifolds we shall adopt the definitions given in C. Chevalley's book [4]. We shall consider exclusively real analytic manifolds, mainly domains in real euclidean spaces, which will be generally denoted by $\mathfrak{V}$. We shall often omit the adjective "real." For a point x in $\mathfrak{V}$, the tangent vector space at x to $\mathfrak{V}$ will be generally denoted by $\mathcal{E}_x\mathfrak{V}$. If $\mathfrak{V}_1$ is a submanifold of $\mathfrak{V}$ and x is in $\mathfrak{V}_1$, $\mathcal{E}_x\mathfrak{V}_1$ is a subspace of $\mathcal{E}_x\mathfrak{V}$. Two submanifolds $\mathfrak{V}_1$ and $\mathfrak{V}_2$ of $\mathfrak{V}$ passing through x are defined to be equivalent at x if there is an open neighborhood N of x in $\mathfrak{V}$ such that $N \cap \mathfrak{V}_1 = N \cap \mathfrak{V}_2$. The equivalence class is called a germ of submanifolds of $\mathfrak{V}$ at x. If a germ contains $\mathfrak{V}_1$, $\mathfrak{V}_1$ is called a representative of the germ. For any germ of submanifolds V at x, the tangent vector space to V, $\mathcal{E}V$, can be defined uniquely as the tangent vector space at x to a representative of V. A subset T in $\mathfrak{V}$ is called a subvariety of $\mathfrak{V}$, if for any point x of T there is an open neighborhood N of x and there is a set K of real analytic functions defined on N such that $T \cap N$ is equal to the common zeros of the functions in K. A subvariety is not necessarily the underlying space of a submanifold. A point x of a subvariety T is called a regular point of T if there is a neighborhood N of x in $\mathfrak{V}$ such that $T \cap N$ is the underlying space of a submanifold. A subvariety T of $\mathfrak{V}$ is called proper if $T \neq \mathfrak{V}$. Remark that the empty set is a proper subvariety. By the classical theorem on the theory of analytic functions, it is clear that a proper subvariety of a (connected) manifold does not contain interior points of the manifold. Let f be an analytic mapping of a manifold $\mathfrak{V}$ onto a manifold $\mathfrak{V}_1$. Assume that for any point x of $\mathfrak{V}_1$ there is an open

neighborhood N of x and an analytic homeomorphism $g: N \times \mathfrak{V}_2 \to f^{-1}(N)$, where $\mathfrak{V}_2$ is a manifold independent of x, such that $(f \circ g)(x', v) = x'$ for any x' in N and v in $\mathfrak{V}_2$, where $f \circ g$ is the composite mapping of f and g. In this case we shall say that f is a fiber mapping.

2. Let $\Lambda\mathfrak{V}$ be the ring of real analytic differential forms on $\mathfrak{V}$. Let $\Lambda^q\mathfrak{V}$ be the module of homogeneous real analytic differential forms of degree q on $\mathfrak{V}$. $\Lambda\mathfrak{V}$ is the direct sum of $\Lambda^0\mathfrak{V}, \Lambda^1\mathfrak{V}, \cdots$, and $\Lambda^n\mathfrak{V}$, where n is the dimension of $\mathfrak{V}$. $\Lambda^0\mathfrak{V}$ is the ring of real analytic functions on $\mathfrak{V}$. The exterior derivative and exterior product would be denoted by d and $\wedge$, respectively. Let θ be a differential form of homogeneous degree q defined on an open set N in $\mathfrak{V}$. By defintion (p. 146 [4]), for each point x of N a q-multilinear function on $\mathcal{E}_x\mathfrak{V}$ is assigned by θ. This function will be denoted by

$$(1) \qquad \langle \theta, \mathcal{E}_x\mathfrak{V} \rangle.$$

If $L_1, \cdots, L_q \in \mathcal{E}_x\mathfrak{V}$, the value of $\langle \theta, \mathcal{E}_x\mathfrak{V} \rangle$ at $L_1, \cdots, L_q$ will be denoted by $\langle \theta, L_1 \wedge \cdots \wedge L_q \rangle$. If $\theta = \theta_1 \wedge \cdots \wedge \theta_q$, then

$$\langle \theta, L_1 \wedge \cdots \wedge L_q \rangle = \det (\langle \theta_i, L_j \rangle).$$

For any subspace E of $\mathcal{E}_x\mathfrak{V}$, the restriction of the function $\langle \theta, \mathcal{E}_x\mathfrak{V} \rangle$ to E will be denoted by

$$(2) \qquad \langle \theta, \mathcal{E} \rangle.$$

Let $\phi_1, \cdots, \phi_h$ be homogeneous differential forms defined on an open set containing x. Let E be a subspace of $\mathcal{E}_x\mathfrak{V}$. If $\langle \phi_1, E \rangle, \cdots, \langle \phi_h, E \rangle$ are linearly independent multilinear functions, we shall say that $\phi_1, \cdots, \phi_h$ are linearly independent on E. If $\phi_1, \cdots, \phi_h$ are linearly independent on $\mathcal{E}_x\mathfrak{V}$, we shall say that $\phi_1, \cdots, \phi_h$ are linearly independent at x.

Let f be an analytic mapping of $\mathfrak{V}$ into $\mathfrak{V}_1$. Let θ be a differential form on an open set N in $\mathfrak{V}_1$. The differential forms on $f^{-1}(N)$ induced by f and θ will be denoted by $f^* \cdot \theta$, ($\delta f \cdot \theta$ by the notations in [4], cf. p. 151 [4]).

3. A q-dimensional subspace of $\mathcal{E}_x\mathfrak{V}$ is called a q-dimensional contact element to $\mathfrak{V}$ at x, and x its origin. The set of all q-dimensional contact elements to $\mathfrak{V}$ at x, $'\mathfrak{G}_x(\mathfrak{V}, q)$, naturally forms an analytic manifold, the so-called Grassmannian manifold. There is a natural analytic manifold structure in $'\mathfrak{G}(\mathfrak{V}, q) = \bigcup \{'\mathfrak{G}_x(\mathfrak{V}, q); x \in \mathfrak{V}\}$ such that $'\mathfrak{G}_x(\mathfrak{V}, q)$ is a submanifold of $'\mathfrak{G}(\mathfrak{V}, q)$ and such that the projection $\rho: {'\mathfrak{G}}(\mathfrak{V}, q) \to \mathfrak{V}$ is an analytic fiber mapping, where ρ maps every contact element to its origin.

4. We shall construct the systems of coordinates of $'\mathfrak{G}(\mathfrak{V}, q)$ which will be used later frequently. Let $\omega^1, \cdots, \omega^q$ be analytic Pfaffian forms defined on a coordinate neighborhood N. Assume that $\omega^1, \cdots, \omega^q$ are linearly independent at each point in N. Set

(3) $$U(\omega^1, \cdots, \omega^q) = \{E \in {}'\mathfrak{G}(\mathfrak{V}, q);\ \rho(E) \in N \text{ and } \omega^1, \cdots, \omega^q \text{ are linearly independent on } E\}.$$

Take analytic Pfaffiian forms $\pi^1, \cdots, \pi^{n-q}$ such that $\omega^1, \cdots, \omega^q, \pi^1, \cdots, \pi^{n-q}$ form a base of Pfaffian forms on N. If $E \in U = U(\omega^1, \cdots, \omega^q)$, there is a unique system of real numbers $a_r^\sigma(E)$, $(r = 1, \cdots . q;\ \sigma = 1, \cdots n - q)$, such that

(4) $$\langle \pi^\sigma, E\rangle - \sum_{r=1}^{q} a_r^\sigma(E) \cdot \langle \omega^r, E\rangle = 0, \qquad (\sigma = 1, \cdots, n - q).$$

The functions a_r^σ are analytic functions on U and $(x^1 \circ \rho, \cdots, x^n \circ \rho, \cdots, a_r^\sigma, \cdots)$ a system of coordinates on U, where $(x^1, \cdots, x^n)$ is a system of coordinates on N. Moreover, this system gives a homeomorphism of U onto $N \times R^{q(n-q)}$, where $R^{q(n-q)}$ is a real euclidean space of $q(n-q)$ dimensions. If E' is in U, E' is equal to the set of all solutions of the following system of linear equations on $\mathcal{E}_{x'}\mathfrak{V}$:

(5) $$\langle \pi^\sigma, \mathcal{E}_{x'}\mathfrak{V}\rangle - \sum_{r=1}^{q} a_r^\sigma(E') \cdot \langle \omega^r, \mathcal{E}_{x'}\mathfrak{V}\rangle = 0, \qquad (\sigma = 1, \cdots, q),$$

where x' is the origin of E'. Let $L_1(E'), \cdots, L_q(E')$ be the tangent vectors in E', defined by the formulas:

(6) $$\langle \omega^s, L_r(E')\rangle = \delta_r^s, \qquad (r, s = 1, \cdots, q),$$

where δ_r^s is Kronecker's delta symbol. Then we have the equality:

(7) $$a_r^\sigma(E') = \langle \pi^\sigma, L_r(E')\rangle.$$

Let $\mathfrak{V}_1$ be a q-dimensional submanifold of $\mathfrak{V}$. The mapping T of $\mathfrak{V}_1$ into $'\mathfrak{G}(\mathfrak{V}, q)$, defined by the formula:

(8) $$T(x) = \mathcal{E}_x\mathfrak{V}_1, \qquad (x \in \mathfrak{V}_1),$$

is regular and locally univalent mapping. Thus T defines a submanifold of $'\mathfrak{G}(\mathfrak{V}, q)$, which will be denoted by $\mathfrak{T}\mathfrak{V}_1$. If V_1 is a germ of q-dimensional submanifolds of $\mathfrak{V}$ at x, we can define the germ of submanifolds TV_1 in $'\mathfrak{G}(\mathfrak{V}, q)$ at $\mathcal{E}V_1$, taking a representative of V_1 and applying T. Define $'\mathfrak{G}^l(\mathfrak{V}, q)$ and $\mathfrak{T}^l\mathfrak{V}_1$, $l = 1, 2, \cdots$, by the inductive formulas:

(8') $$'\mathfrak{G}^1(\mathfrak{V}, q) = {}'\mathfrak{G}(\mathfrak{V}, q),\ {}'\mathfrak{G}^{l+1}(\mathfrak{V}, q) = {}'\mathfrak{G}({}'\mathfrak{G}^l(\mathfrak{V}, q), q),$$
$$\mathfrak{T}^1\mathfrak{V}_1 = \mathfrak{T}\mathfrak{V}_1, \qquad \mathfrak{T}^{l+1}\mathfrak{V}_1 = \mathfrak{T}(\mathfrak{T}^l\mathfrak{V}_1).$$

We can define T^lV_1 by similar formulas. $\mathfrak{J}^l\mathfrak{V}_1$ and T^lV_1 are submanifold and germ of submanifolds, respectively, of $'\mathfrak{G}^l(\mathfrak{V},q)$.

Throughout this paper, let $\mathfrak{V}$ be a (not necessarily bounded) connected domain in the real euclidean space.

Chapter I. Exterior Differential System.

1. Exterior differential system. *Definition* I. 1. An ideal Σ in the ring of real analytic differential forms on $\mathfrak{V}$ is called an exterior differential system if it satisfies the following conditions:

(i) $d\Sigma \subset \Sigma$,

(ii) Σ is homogeneous, i.e., $\Sigma = \Sigma^{[0]} + \Sigma^{[1]} + \cdots + \Sigma^{[n]}$, where $\Sigma^{[i]} = \Sigma \cap \Lambda^i\mathfrak{V}$ and n is the dimension of $\mathfrak{V}$,

(iii) Σ is finitely generated, i.e., there is a finite number of forms $\theta_1, \cdots, \theta_\alpha$ in Σ such that Σ is generated, as an ideal, by $\theta_1, \cdots, \theta_\alpha$.

Let $\phi_1, \cdots, \phi_\beta$ be homogeneous differential forms on $\mathfrak{V}$. The ideal in $\Lambda\mathfrak{V}$ generated by $\phi_1, \cdots, \phi_\beta, d\phi_1, \cdots, d\phi_\beta$ is an exterior differential system, which is called the exterior differential system generated by $\phi_1, \cdots, \phi_\beta$.

Definition I. 2. A (q-dimensional) contact element E to $\mathfrak{V}$ at x is called a (q-dimensional) integral element of Σ if and only if $\langle\theta, E\rangle = 0$ for every θ in Σ (cf. (2)). Let $'\mathfrak{J}^q\Sigma$ be the set of all q-dimensional integral elements of Σ. A zero-dimensional integral element is sometimes called an integral point.

Take linearly independent Pfaffian forms $\omega^1, \cdots, \omega^q$ defined on an open set N. Set $U = U(\omega^1, \cdots, \omega^q)$, (cf. (3)). Then $E \in U$ is an integral element of Σ if and only if

$$(9)\qquad \langle\theta, L_{r_1}(E) \wedge \cdots \wedge L_{r_a}(E)\rangle = 0 \qquad (\theta \in \Sigma^{[a]}; r_1, \cdots, r_a = 1, \cdots, q; a = 0, 1, \cdots, q),$$

where, in the case $a = 0$, the left hand side of (9) means the value of the function θ at the origin of E. Hence, if we define the analytic function $K[\theta, q; r_1, \cdots, r_a]$ on U by the formula:

$$(10)\qquad (K[\theta, q; r_1, \cdots, r_a](E) = \langle\theta, L_{r_1}(E) \wedge \cdots \wedge L_{r_a}(E)\rangle,$$

and denote by $K(\Sigma; \omega^1, \cdots, \omega^q)$ the ideal in the ring $\Lambda^0 U$ of all real analytic functions on U generated by all such $K[\theta, q; r_1, \cdots, r_a]$, then $'\mathfrak{J}^q E \cap U$ is

equal to the set of common zeros of the functions in $K(\Sigma; \omega^1, \cdots, \omega^q)$. Therefore we have the following:

Proposition I. 1. $'\mathfrak{I}^q\Sigma$ is a subvariety of $'\mathfrak{G}(\mathfrak{V}, q)$.

Definition I. 3. Let T be a subvariety of $\mathfrak{V}$ and x be a point of $\mathfrak{V}$. Let K be a set of analytic functions defined on an open neighborhood N of x. The equation $K = 0$ is called a local equation of T at x (or on N) if $N \cap T$ is equal to the set of common zeros of K.

Definition I. 4. The equation: $K(\Sigma, \omega^1, \cdots, \omega^q) = 0$ is called the canonical local equation of $'\mathfrak{I}^q\Sigma$ (on $U(\omega^1, \cdots, \omega^q)$).

Definition I. 5. A submanifold $\mathfrak{V}_1$ of $\mathfrak{V}$ is called an integral manifold of Σ if, for each point x in $\mathfrak{V}_1$ the tangent vector space to $\mathfrak{V}_1$ at x is an integral element of Σ. A germ of submanifolds V_1 in $\mathfrak{V}$ at x is called an integral at x if there is a representative of V_1 which is an integral manifold of Σ.

It is clear that $\mathfrak{V}_1$ is an integral manifold of Σ if and only if the subring Σ_1 of $\Lambda\mathfrak{V}_1$ which is the image of Σ under the dual mapping of the injection of $\mathfrak{V}_1$ into $\mathfrak{V}$ consists of only zero.

2. Polar equations, regular and ordinary integral elements. Let E be a q-dimensional contact element to $\mathfrak{V}$ at x. Any vectors $L_1, \cdots, L_a$ in E and any form θ in $\Sigma^{[a+1]}$ define a linear functional $\theta[L_1, \cdots, L_a]$ on $\mathcal{E}_x\mathfrak{V}$ by the formula:

$$(10') \qquad (\theta[L_1, \cdots, L_a])(L) = \langle \theta, L_1 \wedge \cdots \wedge L_a \wedge L \rangle, \quad (L \in \mathcal{E}_x\mathfrak{V}).$$

$\theta[L_1, \cdots, L_a]$ is equal to $\langle \theta, \mathcal{E}_x\mathfrak{V} \rangle$, when $a = 0$.

Definition I. 6. The subspace of the conjugate space of $\mathcal{E}_x\mathfrak{V}$ generated by all such $\theta[L_1, \cdots, L_a]$, $(\theta \in \Sigma^{[a+1]}; L_1, \cdots, L_a \in E; a = 0, 1, \cdots, q$, will be called the system of polar forms of Σ at E and will be denoted by $J(\Sigma; E)$, (or by $J(E)$). The equation $J(E) = 0$ is called the polar equation of Σ at E. The set of all solutions of this equation will be denoted by $H(E)$.

If E is an integral element of Σ, $H(E)$ contains E. It is easy to see the following:

Proposition I. 2. Let E be an integral element of Σ. Let L be a tangent vector to $\mathfrak{V}$ at the origin of E. Then the subspace spanned by E and L is an integral element of Σ if and only if L is in $H(E)$.

Proposition I. 3. Let $\omega^1, \cdots, \omega^q$ be linearly independent Pfaffian forms

on an open set N. Let $\theta_1, \cdots, \theta_a$ be a system of generators (as an ideal) of Σ. If $E \in U(\omega^1, \cdots, \omega^q)$, the set

$$\{\theta_a[L_{i_1}(E), \cdots, L_{i_d}(E)]\,;\ a = 1, \cdots, \alpha;\ 0 \leqq i_1 \leqq \cdots \leqq i_d \leqq q;\ d = (\text{degree of } \theta_a) - 1 \geqq 0\}$$

is a system of generators of $J(E)$, (cf. (3) and (6)).

The dimension of the vector space $J(E)$ over the field R of real numbers will be denoted by $t(\Sigma; E)$, (or by $t(E)$), where t is considered as an integer valued function on $'\mathfrak{G}(\mathfrak{V}, q)$. If $E' \subseteq E$, the definition implies that $J(E') \subseteq J(E)$. Hence we have

Proposition I. 4. If $E' \subseteq E$, then $t(E') \leqq t(E)$. If $E \in {'\mathfrak{J}^q\Sigma}$, then $t(E) \leqq n - q$.

Definition I. 6. Let E be an element in $'\mathfrak{G}(\mathfrak{V}, q)$. Set

$$t_r(E) = \operatorname{Max}\{t(E')\,; E' \text{ is a } r\text{-dimensional subspace of } E\}. \quad (r = 0, 1, \cdots, q).$$

Proposition I. 4 implies that $t_0(E) \leqq t_1(E) \leqq \cdots \leqq t_q(E) = t(E)$.

Definition I. 7. Let E be an element in $'\mathfrak{G}(\mathfrak{V}, q)$. Define integers $s_0(E), \cdots, s_q(E)$ by the formulas:

$$s_0(E) = t_0(E),\ s_r(E) = t_r(E) - t_{r-1}(E) \qquad (r = 1, \cdots, q-1),$$
$$s_q(E) = n - q - t_{q-1}(E).$$

$s_0(E), \cdots, s_q(E)$ is called the system of characters at E of Σ.

Denote by $\mathfrak{G}(E, r)$ the set of r-dimensional contact elements contained in E. $\mathfrak{G}(E, r)$ is a submanifold of $'\mathfrak{G}(E, r)$.

LEMMA I. 1. *The set of all $E' \in \mathfrak{G}(E, r)$ such that $t(E') \leqq t_r(E)$ is a proper subvariety of $\mathfrak{G}(E, r)$.*

Let T be a subvariety of an analytic manifold $\mathfrak{V}$. Let an equation: $K = 0$ be a local equation of T on an open set N (cf. Definition I. 3).

Definition I. 8. Let x be a point in $N \cap T$. K is called regular at x, if there are functions $f_1, \cdots, f_h$ in K such that the equation: $f_1 = \cdots = f_h = 0$ is a local equation of T on a neighborhood of x and such that $df_1, \cdots, df_h$ are linearly independent at x.

Now we shall define the notions of regular q-dimensional integral element of Σ by induction on q.

Definition I. 9. A point x of $'\mathfrak{J}^0\Sigma$ is called a regular zero-dimensional integral element if and only if there is a neighborhood N of x in $\mathfrak{V}$ such that t is a constant function on $N \cap {'\mathfrak{J}^0\Sigma}$, $N \cap {'\mathfrak{J}^0\Sigma}$ is a submanifold of $\mathfrak{V}$, and the equation $\Sigma^{[0]} = 0$ is a regular local equation of $'\mathfrak{J}^0\Sigma$ on N. A q-dimensional integral element $(q \geqq 1)$, is called regular if and only if

(i) E contains at least one regular $(q-1)$-dimensional integral element,

(ii) there is a neighborhood N of E in $'\mathfrak{G}(\mathfrak{V}, q)$ such that t is a constant function on $N \cap {'\mathfrak{J}^q\Sigma}$.

Definition I. 10. An integral point x is called ordinary if and only if there is a neighborhood N of x in $\mathfrak{V}$ such that $'\mathfrak{J}^0\Sigma \cap N$ is a submanifold and such that the equation: $\Sigma^{[0]} = 0$ on N is a regular local equation of $'\mathfrak{J}^0\Sigma \cap N$. A q-dimensional integral element E $(q \geqq 1)$, is called ordinary if and only if E contains at least one regular $(q-1)$-dimensional integral element.

Definition I. 11. Let E be a q-dimensional vector space. By a flag F on E we mean a chain of subspaces of E,

$$\{0\} = E_0 \subset E_1 \subset \cdots \subset E_r \subset \cdots \subset E_q = E,$$

where the dimension of E_r is r. E_r will be called the r-th component of the flag F. q is called the dimension of F. The set $\mathfrak{F}(E)$ of all flags on E forms a real analytic manifold. There is a natural manifold structure on $\mathfrak{F}(\mathfrak{V}, q) = \bigcup \{F ; F \in \mathfrak{F}(E), E \in {'\mathfrak{G}(\mathfrak{V}, q)}\}$ such that $\mathfrak{F}(E)$ is a submanifold of $\mathfrak{F}(\mathfrak{V}, q)$.

Let F be a flag on $E \in {'\mathfrak{G}(\mathfrak{V}, q)}$. Let N_r be a neighborhood of the r-th component of F in $'\mathfrak{G}(\mathfrak{V}, r)$.

$$(11) \qquad U(N_0, N_1, \cdots, N_q) = \{F' \in \mathfrak{F}(\mathfrak{V}, q) ; \text{ the } r\text{-th component of } F' \text{ is in } N_r,\ r = 0, 1, \cdots, q\}.$$

Then all such $U(N_0, N_1, \cdots, N_q)$ form a fundamental system of neighborhoods of F in $\mathfrak{F}(\mathfrak{V}, q)$.

Definition I. 12. Let E be an ordinary integral element. A flag F on E will be called regular if the r-th component of F is a regular integral element for $r = 0, 1, \cdots, q-1$.

We see easily the following

Proposition I. 5. Let E be an ordinary integral element of Σ. Then

there exists at least one regular flag on E. The set of all regular flags of q dimensions forms an open set in $\mathfrak{F}(\mathfrak{V}, q) \cap \tau^{-1}('\mathfrak{J}^0\Sigma)$, where τ is the natural mapping of $\mathfrak{F}(\mathfrak{V}, q)$ onto $'\mathfrak{G}(\mathfrak{V}, q)$.

Set

(12) $\mathfrak{R}'\mathfrak{J}^q\Sigma = \{E \in {'\mathfrak{G}}(\mathfrak{V}, q)\ ;\ E$ is a regular integral element of $\Sigma\}$

(13) $\mathfrak{O}'\mathfrak{J}^q\Sigma = \{E \in {'\mathfrak{G}}(\mathfrak{V}, q)\ ;\ E$ is an ordinary integral element of $\Sigma\}$.

Clearly we have the relation: $\mathfrak{R}'\mathfrak{J}^q\Sigma \subseteq \mathfrak{O}'\mathfrak{J}^q\Sigma \subseteq {'\mathfrak{J}^q\Sigma}$.

THEOREM I. 1. *$\mathfrak{R}'\mathfrak{J}^q\Sigma$ and $\mathfrak{O}'\mathfrak{J}^q\Sigma$ are open subsets of $'\mathfrak{J}^q\Sigma$. Let E be an ordinary q-dimensional integral element of Σ. Then there is a neighborhood N of the origin of E such that $'\mathfrak{J}^0\Sigma \cap N$ is a submanifold. Let n_0 be the dimension of this submanifold. Let $\omega^1, \cdots, \omega^q$ be analytic Pfaffian forms on N which are linearly independent at each point in N, and which are also linearly independent on E. If N is sufficiently small, then there is a neighborhood $\mathfrak{N}$ of E in $'\mathfrak{G}(\mathfrak{V}, q)$ such that*

(i) *$'\mathfrak{J}^q\Sigma \cap \mathfrak{N}$ is a submanifold of dimension $\left(\sum_{r=1}^{q} r \cdot s_r(E)\right) + n_0$,*

(ii) *the equations $K(\Sigma, \omega^1, \cdots, \omega^q) = 0$ on $\mathfrak{N}$ is a regular local equation of $'\mathfrak{J}^q\Sigma \cap \mathfrak{N}$.*

(iii) *the restriction of the projection ρ on $'\mathfrak{J}^q\Sigma \cap \mathfrak{N}$ is a fiber mapping of $'\mathfrak{J}^q\Sigma \cap \mathfrak{N}$ onto $'\mathfrak{J}^0\Sigma \cap N$.*

The esential part of the theorem is due to Cartan [4]. The present formulation is due to Y. Matsushima (unpublished). This theorem will not be used in the remainder of the present paper.

Remark. $\mathfrak{O}'\mathfrak{J}^q\Sigma$ may be an empty set, even if $'\mathfrak{J}^q\Sigma$ is not empty, as in the following

Example 1. Let $\mathfrak{V}$ be the three-dimensional euclidean space with a system of coordinates (x, y, z). Denote by Σ the exterior system generated by $z \cdot dz$ and $z \cdot dx \wedge dy$. Then $'\mathfrak{J}^2\Sigma \neq \phi$, in fact, $z = 0$ is an integral manifold of Σ. The origin of any 2-dimensional integral element must satisfy the condition: $z = 0$, but such a point is not a regular integral point. Therefore it follows that $\mathfrak{O}'\mathfrak{J}^2\Sigma$ is empty.

The following proposition, which is a corollary of Theorem I. 1 will be used later. Therefore we shall prove it here directly.

Proposition I. 6. Let E be an ordinary q-dimensional integral element

of Σ. Then, we can find a neighborhood N of the origin x of E in $\mathfrak{V}$ such that $N \cap {}'\mathfrak{I}^0\Sigma$ is a submanifold and such that there is an analytic mapping $f\colon N \cap {}'\mathfrak{I}^0\Sigma \to {}'\mathfrak{G}(\mathfrak{V}, q)$ satisfying the following conditions: (i) $f(x) = E$, (ii) $\rho \circ f =$ the identity mapping, and (iii) $f(N \cap {}'\mathfrak{I}^0\Sigma) \subseteq {}'\mathfrak{I}^q\Sigma$.

Proof. By definition, there is a neighborhood N_0 of x such that $N_0 \cap {}'\mathfrak{I}^0\Sigma$ is a submanifold. Let F be a regular flag on E. Let E_r $(r = 0, 1, \cdots, q)$, be the r-th component of F. It is sufficient to show the following statement $(\#)_r$ by induction on r $(r = 0, 1, \cdots, q)$:

$(\#)_r$: There is a neighborhood N_r of x such that $N_r \cap {}'\mathfrak{I}^0\Sigma$ is a submanifold and there is an analytic mapping f_r of $N_r \cap {}'\mathfrak{I}^0\Sigma$ into ${}'\mathfrak{G}(\mathfrak{V}, r)$ such that $f_r(x) = E_r$, $\rho \circ f_r =$ the identity mapping, and such that the image of f_r is in ${}'\mathfrak{I}^r\Sigma$.

$(\#)_0$ is trivial. Assume that $(\#)_{r-1}$ is proved. Let $\omega^1, \cdots, \omega^n$ be a base of Pfaffian forms on N_{r-1}. By Proposition I.3, there are analytic functions A_{bj} $(b = 1, \cdots, h; j = 1, \cdots, n)$, on ${}'\mathfrak{G}(N_{r-1}, r-1)$ such that $\sum_{j=1}^{n} A_{bj}(E') \cdot \langle \omega^j, \mathcal{E}_x\mathfrak{V} \rangle$ $(b = 1, \cdots, h; x' = \rho(E'))$, generate $J(E')$ for any E' in ${}'\mathfrak{G}(N_{r-1}, r-1)$, (cf. Definition I.6). By definition I.9, there is a neighborhood N of E_{r-1} such that the dimension of $J(E')$ is constant when E' runs through N. Take a vector L in E_r but not in E_{r-1}. Then it follows that there is an analytic mapping $g\colon f_{r-1}(N_r \cap {}'\mathfrak{I}^0\Sigma) \to \mathcal{E}\mathfrak{V}$ (= the manifold of all tangent vectors to $\mathfrak{V}$) such that $\rho \circ g \circ f_{r-1} =$ the identity, $g(E_{r-1}) = L$, and such that $g(E') \in H(E')$ for any E' in $f_{r-1}(N_r \cap {}'\mathfrak{I}^0\Sigma)$, where N_r is a sufficiently small neighborhood of x contained in N_{r-1}. Adopting the system of coordinates mentioned in the preliminaries, we see easily that the mapping f_r of $N_r \cap {}'\mathfrak{I}^0\Sigma$ into ${}'\mathfrak{G}(\mathfrak{V}, r)$, defined by the formula: $f_r(x') = \{$the subspace spanned by $f_{r-1}(x')$ and $g \circ f_{r-1}(x')\}$, has the required properties.

3. E. Cartan's fundamental theorem.

THEOREM I.2. *Let Σ be an exterior differential system on $\mathfrak{V}$. Let V_1 be an integral of Σ at x (Definition* I.5). *Assume that $\mathcal{E}V_1 = E'$ is a regular integral element of Σ. Let E be a p-dimensional integral element of Σ, where $p-1$ is the dimension of V_1. Let V_2 be a germ of submanifolds in $\mathfrak{V}$. Suppose that they satisfy the following conditions:* (i) $E' \subset E$, (ii) *the dimension of $V_2 = n - s_{p-1}(E') + 1$, where n is the dimension of $\mathfrak{V}$,* (iii) $V_1 \subset V_2$, *and* (iv) $\mathcal{E}V_2 \cap H(E') = E$. *Then for any such E and V_2, there is a unique integral V_3 of Σ at x such that $\mathcal{E}V_3 = E$ and such that $V_1 \subset V_3 \subset V_2$.*

The theorem was first proved by E. Cartan, in the case Σ is generated as an ideal by $\Sigma^{[0]}$, $\Sigma^{[1]}$, and $\Sigma^{[2]}$. The general case was proved by E. Kähler [5]. The formulation of the theorem given here is due to E. Kähler.

Definition I. 13. An integral V_1 of Σ (at x) is called a general solution of Σ (at x) if $\mathcal{E}V_1$ is an ordinary integral element of Σ.

Remark 1. Theorem I. 2 (and its proof) provides an effective method to construct all general solutions at a regular integral point. The theorem is classically expressed by saying that, for any $(p-1)$-dimensional integral V_1 of Σ such that $\mathcal{E}V_1$ is a regular integral element and for any p-dimensional integral element E containing $\mathcal{E}V_1$, the set of all integrals whose tangent vector space is E, depends on $s_{p-1}(\mathcal{E}V_1)-1$ number of arbitrary functions of p variables. But it seems to the writer that some ambiguous points are left open about this notion.

4. Exterior differential system with independent variables.

Definition I. 14. A $\Lambda^0\mathcal{V}$-submodule Ω of $\Lambda^1\mathcal{V}$ is called a system of p independent variables if it satisfies the following conditions: there are analytic functions $f_1,\cdots,f_p$ on $\mathcal{V}$ such that $\omega^1=df_1,\cdots,\omega^p=df_p$ are linearly independent at each point in $\mathcal{V}$ and such that Ω is $\Lambda^0\mathcal{V}$-generated by $df_1,\cdots,df_p$. The set $\{\omega^1,\cdots,\omega^p\}$ is called a base of Ω.

Let n be the dimension of $\mathcal{V}$. Then $\Lambda^1\mathcal{V}$ itself is a system of n independent variables (since $\mathcal{V}$ is a domain in a euclidean space).

Proposition I. 7. Let f be an analytic mapping of $\mathcal{V}$ onto $\mathcal{V}_1$. Let Ω be a system of p independent variables on $\mathcal{V}_1$. Let $f^*\Omega$ be the $\Lambda^0\mathcal{V}$-submodule generalted by all $f^*\omega$, where ω runs through the forms in Ω. Then $f^*\Omega$ is a system of p independent variables on $\mathcal{V}$.

Set

$$(14)\qquad \mathcal{G}_\Omega(\mathcal{V},q)=\{E\in{}'\mathcal{G}(\mathcal{V},q)\,;\text{ the dimension of the vector space }\langle\Omega,E\rangle\text{ is equal to }q\}.$$

Then $\mathcal{G}_\Omega(\mathcal{V},q)$ is an open submanifold of $'\mathcal{G}(\mathcal{V},q)$. Let f be an analytic mapping of $\mathcal{V}_1$ onto $\mathcal{V}$. Then f induces an analytic mapping

$$(15)\qquad d_qf:\ \mathcal{G}_{f^*\Omega}(\mathcal{V}_1,q)\to\mathcal{G}_\Omega(\mathcal{V},q).$$

We shall write simply $\mathcal{G}(\mathcal{V},q)$ instead of $\mathcal{G}_\Omega(\mathcal{V},q)$, when there is no ambiguity about what a system of independent variables is considered.

Definition I. 15. A pair of exterior differential system Σ on $\mathfrak{V}$ and a system of p independent variables Ω on $\mathfrak{V}$ is called an exterior differential system with p independent variables and will be denoted by (Σ, Ω). p is called the number of independent variables in (Σ, Ω).

Definition I. 16. A q-dimensional integral element E of Σ is called an integral element of (Σ, Ω), if E is in $\mathfrak{G}_\Omega(\mathfrak{V}, q)$. By an integral manifold of (Σ, Ω), we mean a p-dimensional integral manifold $\mathfrak{V}_1$ of (Σ, Ω) such that $\mathcal{E}_x\mathfrak{V}_1$ is an integral element of (Σ, Ω) for each x in $\mathfrak{V}_1$, where p is the number of independent variables in Ω. A germ of submanifolds is called an integral of (Σ, Ω) if it contains a representative which is an integral manifold of (Σ, Ω).

Set

$$\mathfrak{I}^q(\Sigma, \Omega) = {}'\mathfrak{I}^q\Sigma \cap \mathfrak{G}_\Omega(\mathfrak{V}, q), \tag{16}$$

$$\mathfrak{O}\mathfrak{I}^q(\Sigma, \Omega) = \mathfrak{O}'\mathfrak{I}^q\Sigma \cap \mathfrak{G}_\Omega(\mathfrak{V}, q), \tag{17}$$

$$\mathfrak{R}\mathfrak{I}^q(\Sigma, \Omega) = \mathfrak{R}'\mathfrak{I}^q\Sigma \cap \mathfrak{G}_\Omega(\mathfrak{V}, q). \tag{18}$$

Since $\mathfrak{G}_\Omega(\mathfrak{V}, q)$ is an open submanifold of $'\mathfrak{G}(\mathfrak{V}, q)$, Proposition I. 1 implies that $\mathfrak{I}^q(\Sigma, \Omega)$ is a subvariety of $\mathfrak{G}_\Omega(\mathfrak{V}, q)$.

Let E be a contact element to $\mathfrak{V}$ at x. $J(\Sigma; E)$ and $\langle \Omega, \mathcal{E}_x\mathfrak{V}\rangle$ are subspaces of the vector space $\langle \Lambda^1\mathfrak{V}, \mathcal{E}_x\mathfrak{V}\rangle = (\mathcal{E}_x\mathfrak{V})'$ (cf. Definition I. 6). Let f be the natural mapping of $(\mathcal{E}_x\mathfrak{V})'$ onto $(\mathcal{E}_x\mathfrak{V})'/\langle \Omega, \mathcal{E}_x\mathfrak{V}\rangle$. Denote by $J(\Sigma, \Omega; E)$ the image of $J(\Sigma, E)$ by f. $J(\Sigma, \Omega; E)$ is called the system of reduced polar forms of E. The dimension of $J(\Sigma, \Omega; E)$ will be denoted by $t(\Sigma, \Omega; E)$ (or by $t(E, \Omega)$). If $E' \subseteq E$, then it follows that $t(E'; \Omega) \leqq t(E; \Omega)$.

Definition I. 6′. Let E be an element in $\mathfrak{G}_\Omega(\mathfrak{V}, q)$. Set $t_r(E) = \operatorname{Max}\{t(E', \Omega)$; E' is a r-dimensional subspace of $E\}$, $(r = 0, 1, \cdots, q)$. Then $t_0(E, \Omega) \leqq t_1(E, \Omega) \leqq \cdots \leqq t_q(E, \Omega) = t(E, \Omega)$.

Definition I. 7′. Let E be an element in $\mathfrak{G}_\Omega(\mathfrak{V}, q)$. Define integers $s_0(E, \Omega), \cdots, s_q(E, \Omega)$ by the formulas:

$$\begin{aligned} s_0(E, \Omega) &= t_0(E, \Omega), \\ s_r(E, \Omega) &= t_r(E, \Omega) - t_{r-1}(E, \Omega), \qquad (r = 1, \cdots, q-1), \\ s_q(E, \Omega) &= n - q - t_{q-1}(E, \Omega). \end{aligned}$$

$s_0(E, \Omega), \cdots, s_q(E, \Omega)$ is called the system of reduced characters at E of (Σ, Ω).

Definition I. 17. Let (Σ, Ω) be an exterior differential system with p independent variables. Let x be an integral point of (Σ, Ω). (Σ, Ω) is called involutive at x if it satisfies the following conditions: (i) $\mathfrak{J}^p(\Sigma, \Omega) \cap \rho^{-1}(x)$ is not empty, (ii) $\mathfrak{J}^p(\Sigma, \Omega) \cap \rho^{-1}(x) \subseteq \mathfrak{O}\mathfrak{J}^p(\Sigma, \Omega)$.

5. Prolongations of exterior differential systems. Let Ω be a system of p independent variables on $\mathfrak{V}$. We shall write simply $\mathfrak{G}(\mathfrak{V}, p)$ instead of $\mathfrak{G}_\Omega(\mathfrak{V}, p)$. We remark that $\mathfrak{G}(\mathfrak{V}, p)$ is again a domain in the euclidean space of $n + p(n-p)$ dimensions (cf. 4. Preliminaries). Let ρ be the projection of $\mathfrak{G}(\mathfrak{V}, p)$ onto $\mathfrak{V}$. Denote by $\rho^* \cdot \Lambda^1\mathfrak{V}$ the $\Lambda^0\mathfrak{G}(\mathfrak{V}, p)$-submodule of $\Lambda^1\mathfrak{G}(\mathfrak{V}, p)$ generated by all $\rho^* \cdot \theta$, where θ runs through forms in $\Lambda^1\mathfrak{V}$. $\Lambda^0\mathfrak{G}(\mathfrak{V}, p)$ is, according to our general notations, the ring of real analytic functions on $\mathfrak{G}(\mathfrak{V}, p)$. Let E be an element in $\mathfrak{G}(\mathfrak{V}, p)$. Let L be a tangent vector to $\mathfrak{G}(\mathfrak{V}, p)$ at E (i.e., $L \in \mathcal{E}_E\mathfrak{G}(\mathfrak{V}, p)$). If $d\rho \cdot L = 0$ and if ψ is in $\rho^*\Lambda^1\mathfrak{V}$, then clearly $\langle \psi, L \rangle = 0$. Therefore a linear functional $\langle \psi . \mathcal{E}_x\mathfrak{V} \rangle_E$ on $\mathcal{E}_x\mathfrak{V}$, where x is the origin of E, is defined by the formula: $\langle \psi, \mathcal{E}_E\mathfrak{G}(\mathfrak{V}, p) \rangle = \langle \psi, \mathcal{E}_x\mathfrak{V} \rangle_E \circ d\rho$. The restriction of $\langle \psi, \mathcal{E}_x\mathfrak{V} \rangle_E$ to a subspace E' of $\mathcal{E}_x\mathfrak{V}$ will be denoted by $\langle \psi, E' \rangle_E$. If we write $\psi = \sum_{j=1}^{k} g_j \cdot \rho^*\theta^j$, where g_j are analytical functions on $\mathfrak{G}(\mathfrak{V}, p)$ and θ^j are analytic Pfaffian forms on $\mathfrak{V}$, then clearly $\langle \psi, E' \rangle_E = \sum_{j=1}^{k} g_j(E) \cdot \langle \theta^j, E' \rangle$. We shall write $\langle \psi, E \rangle$ instead of $\langle \psi, E \rangle_E$.

Definition I. 18. Denote by $\Pi^{[1]}\Omega$ the set of all ψ in $\rho^*\Lambda^1\mathfrak{V}$ such that $\langle \psi, E \rangle = 0$ for all E in $\mathfrak{G}(\mathfrak{V}, p) = \mathfrak{G}_\Omega(\mathfrak{V}, p)$. Denote by $\Pi\Omega$ the ideal in $\Lambda\mathfrak{G}(\mathfrak{V}, p)$ generated by $\Pi^{[1]}\Omega$ and $d(\Pi^{[1]}\Omega)$. We shall see that $\Pi\Omega$ is an exterior differential system on $\mathfrak{G}(\mathfrak{V}, p)$. The exterior differential system with independent variables $(\Pi\Omega, \rho^*\Omega)$ will be called the associated differential system with Ω.

Let $\omega^1 = df_1, \cdots \omega^p = df_p$ be a base of Ω. Then it is obvious that $U(\omega^1, \cdots, \omega^p)$ (cf. (3)), is equal to $\mathfrak{G}(\mathfrak{V}, p)$. Therefore, if we choose analytic Pfaffian forms $\pi^1, \cdots, \pi^{n-p}$ such that $\omega^1, \cdots, \omega^p, \pi^1, \cdots, \pi^{n-p}$ form a base of $\Lambda^1\mathfrak{V}$, we may define a_i^σ, $(i = 1, \cdots, p;\ \sigma = 1, \cdots, n-p)$, on $\mathfrak{G}(\mathfrak{V}, p)$ by formula (4).

Proposition I. 8. $\Pi^{[1]}\Omega$ is generated by $\rho^*\pi^\sigma - \sum_{i=1}^{p} a_i^\sigma \cdot \rho^*\omega^i$, $(\sigma = 1, \cdots, n-p)$.

Proof. Any ψ in $\rho^*\Lambda^1\mathfrak{V}$ can be written as $\psi = g_1 \cdot \rho^*\omega^1 + \cdots + g_p \cdot \rho^*\omega^p$

$+h_1\cdot\rho^*\pi^1+\cdots+h_{n-p}\cdot\rho^*\pi^{n-p}$, where g_i and h_σ are analtyic functions on $\mathfrak{G}(\mathfrak{V},p)$. ψ is in $\Pi^{[1]}\Omega$ if and only if

$$0=\sum_{i=1}^{p}g_i(E)\cdot\langle\omega^i,E\rangle+\sum_{\sigma=1}^{n-p}h_\sigma(E)\cdot\langle\pi^\sigma,E\rangle$$

$$=\sum_{i=1}^{p}(g_i(E)+\sum_{\sigma=1}^{n-p}h_\sigma(E)\cdot a_i^\sigma(E))\langle\omega^i,E\rangle$$

for any E in $\mathfrak{G}(\mathfrak{V},p)$. Therefore $g_i=-\sum_{\sigma=1}^{n-p}h_\sigma\cdot a_i^\sigma$. Thus ψ is in $\Pi^{[1]}\Omega$ if and only if $\psi=\sum_{\sigma=1}^{n-p}h_\sigma\cdot(\rho^*\pi^\sigma-\sum_{i=1}^{p}a_i^\sigma\cdot\rho^*\omega^i)$.

Proposition I.8 implies, in particular, that $\Pi\Omega$ is an exterior differential system.

THEOREM I.3. *Let Ω be a system of p independent variables. If $\mathfrak{V}_1$ is a p-dimensional submanifold of $\mathfrak{V}$ such that $\mathcal{E}_x\mathfrak{V}_1\in\mathfrak{G}(\mathfrak{V},p)$ for any x in $\mathfrak{V}_1$, then $\mathcal{J}\mathfrak{V}_1$ (cf. (8)) is an integral manifold of $(\Pi\Omega,\rho^*\Omega)$. Conversely, if V_1^* is an integral of $(\Omega\Pi,\rho^*\Omega)$, then there is a unique germ of submanifolds $\mathfrak{V}_1$ of $\mathfrak{V}$ such that $\mathcal{J}\mathfrak{V}_1=\mathfrak{V}^*$.*

Proof. The first half of the theorem is almost obvious by the formula (4) and Proposition I.8. As for the second half, let $\mathfrak{V}_1^*$ be an integral manifold of $(\Pi\Omega,\rho^*\Omega)$. Then if E is in $\mathfrak{V}_1^*$, then $\langle\pi^\sigma,d\rho\cdot(\mathcal{E}_E\mathfrak{V}_1^*)\rangle-\sum_{i=1}^{p}a_i^\sigma(E)\cdot\langle\omega^i,d\rho\cdot(\mathcal{E}_E\mathfrak{V}_1^*)\rangle=0$. By (5), it follows that $d\rho\cdot(\mathcal{E}_E\mathfrak{V}_1^*)\subseteq E$. Since $\mathcal{E}_E\mathfrak{V}_1^*$ is in $\mathfrak{G}_{\rho^*\Omega}(\mathfrak{G}(\mathfrak{V},p),p)$, it follows that $d\rho\cdot(\mathcal{E}_E\mathfrak{V}_1^*)$ is p-dimensional. Hence $d\rho\cdot(\mathcal{E}_E\mathfrak{V}_1^*)=E$. And locally $d\rho$ is univalent. Therefore $\rho:\mathfrak{V}_1^*\to\mathfrak{V}$ defines a submanifold $\mathfrak{V}_1$ of $\mathfrak{V}$. For any E in $\mathfrak{V}_1^*$, $\mathcal{E}_{\rho(E)}\mathfrak{V}_1=d\rho\cdot(\mathcal{E}_E\mathfrak{V}_1^*)=E$. Thus $\mathfrak{V}_1^*=\mathcal{J}\mathfrak{V}_1$. In the above proof, $\mathfrak{V}_1$ is not a submanifold in the strict sense, because $d\rho$ is only locally univalent. But what matters here is the germs determined by $\mathfrak{V}_1^*$. Therefore this point does not matter in this proof.

Let $\omega^1,\cdots,\omega^p$ be a base of Ω. Then the ideal $K(\Sigma;\omega^1,\cdots,\omega^p)$, (cf. (10)), in the ring of analytic functions on $U(\omega^1,\cdots,\omega^p)=\mathfrak{G}(\mathfrak{V},p)$ does not depend on the choice of the base. Let us denote this ideal by $K(\Sigma,\Omega)$. We showed that $K(\Sigma,\Omega)$ is finitely generated. Let $\mathfrak{P}_\Omega\Sigma$ be the exterior differential system on $\mathfrak{G}_\Omega(\mathfrak{V},p)=\mathfrak{G}(\mathfrak{V},p)$ generated by $K(\Sigma,\Omega)$ and $\Pi\Omega$.

Definition I.19. *Let* (Σ,Ω) be an exterior differential system with independent variables on $\mathfrak{V}$. The exterior differential system with independent variables $(\mathfrak{P}_\Omega\Sigma,\rho^*\Omega)$ on $\mathfrak{G}_\Omega(\mathfrak{V},p)$ is called the prolongation of (Σ,Ω), and

will be denoted by $\mathfrak{P}(\Sigma,\Omega)$. The l-th iteration of prolongations will be denoted by $\mathfrak{P}^l(\Sigma,\Omega)$.

Proposition I. 9. $'\mathfrak{J}^0\mathfrak{P}_\Omega\Sigma = \mathfrak{J}^p(\Sigma,\Omega)$, where p is the number of independent variables in (Σ,Ω).

The proof is obvious by the definitions.

THEOREM I. 4. *Let (Σ,Ω) be an exterior differential system with independent variables. If $\mathfrak{V}_1$ is an integral manifold of (Σ,Ω), $\mathcal{T}\mathfrak{V}_1$ is an integral manifold of $\mathfrak{P}(\Sigma,\Omega)$. Conversely, if $\mathfrak{V}_1{}^*$ is an integral of $\mathfrak{P}(\Sigma,\Omega)$, there is a unique germ of submanifolds $\mathfrak{V}_1$ of $\mathfrak{V}$ such that $\mathcal{T}\mathfrak{V}_1 = \mathfrak{V}^*$. Then $\mathfrak{V}_1$ is automatically an integral manifold of (Σ,Ω).*

Proof. Let $\mathfrak{V}_1$ be an integral manifold of (Σ,Ω). Then $\mathcal{T}\mathfrak{V}_1 \subseteq {}'\mathfrak{J}^0\mathfrak{P}_\Omega\Sigma = \mathfrak{J}^p(\Sigma,\Omega)$, where p is the number of independent variables. By Theorem I. 3, $\mathcal{T}\mathfrak{V}_1$ is an integral manifold of $(\Pi\Omega, \rho^*\Omega)$. Then it follows that $\mathcal{T}\mathfrak{V}_1$ is an integral manifold of $\mathfrak{P}(\Sigma,\Omega)$. Let $\mathfrak{V}_1{}^*$ be an integral manifold of $\mathfrak{P}(\Sigma,\Omega)$. Then $\mathfrak{V}_1{}^*$ is an integral manifold of $(\Pi\Omega,\rho^*\Omega)$. Therefore, by Theorem I. 3, there is a unique submanifold $\mathfrak{V}_1$ of $\mathfrak{V}$ such that $\mathcal{T}\mathfrak{V}_1 = \mathfrak{V}_1{}^*$. Since $\mathcal{T}\mathfrak{V}_1 = \mathfrak{V}_1{}^* \subseteq {}'\mathfrak{J}^0\mathfrak{P}_\Omega\Sigma = \mathfrak{J}^p(\Sigma.\Omega)$, $\mathfrak{V}_1$ is an integral manifold of (Σ,Ω). Here we assumed that $\mathfrak{V}_1{}^*$ is a sufficiently small representative of $V_1{}^*$.

THEOREM I. 5. *Let (Σ,Ω) be an exterior differential system with p independent variables on $\mathfrak{V}$. Let E^* be a p-dimensional integral element of $\mathfrak{P}(\Sigma,\Omega)$. If, moveover, $d\rho\cdot E^*$ is an ordinary integral element, we have the following relations:*

$$s_q(E^*) = \sum_{r=q}^{p} s_r(E), \qquad (E = d\rho\cdot E^*;\ q = 1,\cdots,p).$$

This theorem was proved by E. Cartan [2] in the case where Σ is generated by $\Sigma^{[0]}$, $\Sigma^{[1]}$, and $d\Sigma^{[1]}$. The general case was proved by Y. Matsushima [6].

Remark. The theorem shows that, if E is an ordinary integral element of (Σ,Ω), any integral element E^* of $\mathfrak{P}(\Sigma,\Omega)$ such that $d\rho\cdot E^* = E$ is ordinary. But the ordinarity of E^* does not imply that of E.

The following lemma, which is easy to prove, is often useful in calculating prolongations.

LEMMA I. 2. *Let (Σ,Ω) be exterior differential system. Let $\omega^1,\cdots,\omega^p$ be a base of Ω. Then the functions $K[\theta,p;r_1,\cdots,r_a] = K_{r_1\cdots r_a}$ on*

$\mathfrak{G}_\Omega(\mathfrak{V},p)=U(\omega^1,\cdots,\omega^p)$, *defined by formula* (10), *where a is the degree of the differential form* θ, *are uniquely determined by the following formula*:

$$\rho^*\theta\equiv\sum_{1\leqq r_1<\cdots<r_a\leqq p}K_{r_1\cdots r_a}\cdot\rho^*\omega^{r_1}\wedge\cdots\wedge\rho^*\omega^{r_a}\qquad(\mathrm{mod}\,\Pi^{[1]}\Omega).\tag{19}$$

Chapter II. Normal Exterior Differential System.

1. Normal exterior differential system.

Definition II. 1. An exterior differential system with independent variables (Σ,Ω) on a real analytic manifold $\mathfrak{V}$ is called normal if it satisfies the following conditions

(i) $\Sigma^{[0]}=0$;

(ii) there are analytic Pfaffian forms $\theta^1,\cdots,\theta^{\alpha_1}$ on $\mathfrak{V}$ which form a system of generators of $\Sigma^{[1]}$ and which are linearly independent modulo Ω at each point in $\mathfrak{V}$;

(iii) $\Sigma^{[2]}\equiv 0$; $(\mathrm{mod}\,\Omega+\Sigma^{[1]})$

(iv) Σ is generated as an ideal by $\Sigma^{[1]}$ and $\Sigma^{[2]}$.

THEOREM II. 1. *Let* (Σ,Ω) *be an exterior system with p independent variables on* $\mathfrak{V}$. *Then* $\mathfrak{P}(\Sigma,\Omega)$ *satisfies the conditions* (iii) *and* (iv) *in Definition* II. 1.

Therefore, if $\mathfrak{I}^p(\Sigma,\Omega)$ forms a submanifold on a neighborhood N of a p-dimensional element, restricting $\mathfrak{P}(\Sigma,\Omega)$ on N, we may obtain in general a normal exterior system with independent variables. For this reason, we shall restrict our attention to a normal exterior differential system with independent variables. Of course, there are many systems which cannot be treated by the theory of normal systems. We shall say simply normal system instead of normal exterior differential system with independent variables.

Our next concern is to express $\mathfrak{P}^l(\Sigma,\Omega)$ more explicitly. To do this we shall restrict $\mathfrak{P}^l(\Sigma,\Omega)$ on a submanifold of $\mathfrak{G}^l(\mathfrak{V},p)$ which contains $\mathfrak{I}^0\mathfrak{P}^l(\Sigma,\Omega)$, and we shall write down explicitly the systems and their systems of polar forms.

2. Admissible restriction.

Let Σ be an exterior differential system on $\mathfrak{V}$. Let $f_1,\cdots,f_c$ be analytic functions in $\Sigma^{[0]}$ such that $df_1,\cdots,df_c$ are linearly independent at each point in $\mathfrak{V}$. Let $\mathfrak{V}'$ be the submanifold of

$\mathfrak{V}$ defined by the conditions: $f_1 = \cdots = f_c = 0$. Σ induces an exterior differential system Σ' on $\mathfrak{V}'$. Σ' is called an admissible restriction of Σ and c is called the character of the admissible restriction. Let Ω be a system of p independent variables on $\mathfrak{V}$. Denote by Ω' the $\Lambda^0\mathfrak{V}'$-submodule generated by the restriction of Ω to $\mathfrak{V}'$. If Ω' is a system of p independent variables, we shall say that (Σ', Ω') is an admissible restriction of (Σ, Ω), and that c is the character of the restriction.

Proposition II. 1. Let (Σ', Ω') on $\mathfrak{V}'$ be an admissible restriction of (Σ, Ω) on $\mathfrak{V}$. For $q = 0, 1, \cdots, \dim \mathfrak{V}$, denote by i_q the injection of $\mathfrak{G}_{\Omega'}(\mathfrak{V}', q)$ into $\mathfrak{G}_{\Omega}(\mathfrak{V}, q)$ induced by the injection i of $\mathfrak{V}'$ into $\mathfrak{V}$. Then i_q induces a homeomorphism of $\mathfrak{I}^q(\Sigma', \Omega')$ onto $\mathfrak{I}^q(\Sigma, \Omega)$. If E is an element of $\mathfrak{I}^q(\Sigma', \Omega')$, then $s_0(i_q(E)) + c = s_0(E)$ and $s_r(i_q(E)) = s_r(E)$ for $r = 1, \cdots, q$, where c is the character of the restriction.

Proof. Let (Σ', Ω') be an admissible restriction by the functions $f_1, \cdots, f_c$ in $\Sigma^{[0]}$. The first half of the proposition follows from the fact that f_j and df_j, $(j = 1, \cdots, c)$, are in Σ. Let x be an integral point of Σ'. Let i^* be the linear mapping of $\langle \Lambda^1\mathfrak{V}, \mathcal{E}_x\mathfrak{V}\rangle$ onto $\langle \Lambda^1\mathfrak{V}', \mathcal{E}_x\mathfrak{V}'\rangle$ induced by i. Then the kernel of i^* is the subspace generated by $\langle df_1, \mathcal{E}_x\mathfrak{V}\rangle, \cdots \langle df_c, \mathcal{E}_x\mathfrak{V}\rangle$. Hence $t(\Sigma', x) + c = t(\Sigma, i(x))$. Assume that $t(\Sigma', E_1) + c = t(\Sigma, i(E_1))$ for any E_1 in $\mathfrak{G}_{\Omega}(\mathfrak{V}', r)$ for $r = 1, \cdots, q-1$. Let E be an element in $\mathfrak{G}_{\Omega}(\mathfrak{V}, q)$. Take a $(q-1)$-dimensional subspace E_1 of E. Then i^* induces a mapping $J(i(E))/J(i(E_1))$ onto $J(E)/J(E_1)$. The kernel of i^* is in $J(\Sigma, i(x)) \subseteq J(\Sigma, i(E_1))$, where x is the origin of E. Hence

$$J(\Sigma, i(E))/J(\Sigma, i(E_1)) \approx J(\Sigma', E)/J(\Sigma', E_1).$$

Therefore, using the assumption of induction, we see that $t(\Sigma', E) + c = t(\Sigma, i(E))$. Then, by Definition I. 7, we can easily deduce the second half of the proposition.

Proposition II. 2. Let (Σ', Ω') on $\mathfrak{V}'$ be an admissible restriction of (Σ, Ω) on $\mathfrak{V}$. Let c be the character of the restriction. We can naturally identify $\mathfrak{G}_{\Omega'}(\mathfrak{V}', p)$ to a submanifold of $\mathfrak{G}_{\Omega}(\mathfrak{V}, p)$, where p is the number of independent variables. Then $\mathfrak{P}(\Sigma', \Omega')$ is an admissible restriction of $\mathfrak{P}(\Sigma, \Omega)$ and its character is equal to $c(p+1)$.

Proof. Let $\omega^1, \cdots, \omega^p$ be a base of Ω. Then $\mathfrak{G}_{\Omega}(\mathfrak{V}, p) = U(\omega^1, \cdots, \omega^p)$. To construct a system of coordinates on $U(\omega^1, \cdots, \omega^p)$, we can choose $\pi^1, \cdots, \pi^{n-p}$ such that $\pi^1 = df_1, \cdots, \pi^c = df_c$ (cf. **4.** in Preliminaries). Then $\mathfrak{G}_{\Omega'}(\mathfrak{V}', p)$ is the submanifold defined by the system of equations (*):

$f_1 = \cdots = f_c = a_r{}^j = 0$ $(r = 1, \cdots, p: j = 1, \cdots, c)$. Since df_j is in $\Sigma^{[1]}$, the functions $a_r{}^j$ are in $\mathcal{P}(\Sigma, \Omega)$. Hence (*) defines an admissible restriction $\mathcal{P}(\Sigma, \Omega)'$ of $\mathcal{P}(\Sigma, \Omega)$ and its character is $c(p+1)$. It remains to prove that $\mathcal{P}(\Sigma, \Omega)' = \mathcal{P}(\Sigma', \Omega')$. This can be done by writing down the elements in $\mathcal{P}(\Sigma', \Omega')$ and $\mathcal{P}(\Sigma, \Omega)'$.

Proposition II. 3. Let (Σ', Ω') be an admissible restriction of (Σ, Ω). Let (Σ'', Ω'') be an admissible restriction of (Σ', Ω'). Let c' and c'' be their characters. Then (Σ'', Ω'') is an admissible restriction of (Σ, Ω) and its character is $c' + c''$.

The proof is easy.

3. The exterior differential system $\mathcal{R}_l\Sigma$. Let (Σ, Ω) be a normal system on $\mathcal{V}$. Let $\omega^1, \cdots, \omega^p$ be a base of Ω. Remark that $d\omega^i = 0$ by Definition I. 14. We can choose a base $\omega^1, \cdots, \omega^p, \theta^1, \cdots, \theta^{\alpha_1}, \varpi^1, \cdots, \varpi^m$ of Pfaffian forms on $\mathcal{V}$ such that $\theta^1, \cdots, \theta^{\alpha_1}$ generate $\Sigma^{[1]}$, and $d\varpi^\lambda = 0$. Throughout § 2 and § 3, we shall fix a base. Let $u^\lambda{}_{i_1 \cdots i_l}$, $(\lambda = 1, \cdots, m;$ $i_1, \cdots, i_l = 1, \cdots, p;$ $l = 1, 2, \cdots)$, be a system of indeterminates under the conditions: $u^\lambda{}_{i_1 \cdots i_l} = u^\lambda{}_{j_1 \cdots j_l}$, where $j_1, \cdots, j_l$ is any permutation of $i_1, \cdots, i_l$. We can consider $u^\lambda{}_{i_1 \cdots i_l}$, for a fixed l, as a system of coordinates in euclidean space R_l of dimension $n_l = m \cdot C_l{}^{p+l-1}$, where $C_b{}^a$ is the binomial coefficient. Set $R_0 = \mathcal{V}$ and $n_0 =$ the dimension of $\mathcal{V}$.

Set $\mathcal{R}_l = R_0 \times R_1 \times \cdots \times R_l$ $(l \geqq 0)$. We have the projection $\rho_{l'}{}^l$: $\mathcal{R}_l \to \mathcal{R}_{l'}$ for $l \geqq l'$. To avoid inessential complications of notations, let us omit the symbols $\circ \rho_{l'}{}^l$, $(\rho_{l'}{}^l)^*$, as far as confusion may not occur. For example, if f is a function on $\mathcal{R}_{l'}$, f automatically means also the functions $f \circ \rho_{l'}{}^l$ on $\mathcal{R}_l$ for any $l \geqq l'$. The same rule will be applied to differential forms. When we want to indicate on what manifold f is considered, we shall say f on $\mathcal{R}_l$, for example.

Let Π_l be the $\Lambda^0\mathcal{R}_l$-submodule of $\Lambda^1\mathcal{R}_l$ generated by the following set (Π_l) of Pfaffian forms on $\mathcal{R}_l$:

$$
(\Pi_l) \quad
\begin{aligned}
&\theta^\alpha, \quad (\alpha = 1, \cdots, \alpha_1), \\
&{}^*\varpi^\lambda = \varpi^\lambda - \sum_{i=1}^{p} u^\lambda{}_i \cdot \omega^i, \quad {}^*\varpi^\lambda{}_{k_1} = du^\lambda{}_{k_1} - \sum_{i=1}^{p} u^\lambda{}_{k_1 i} \cdot \omega^i, \cdots, \\
&{}^*\varpi^\lambda{}_{k_1 \cdots k_\nu} = du^\lambda{}_{k_1 \cdots k_\nu} - \sum_{i=1}^{p} u^\lambda{}_{k_1 \cdots k_\nu i} \cdot \omega^i, \cdots, \\
&\varpi^\lambda{}_{k_1 \cdots k_{l-1}} = du^\lambda{}_{k_1 \cdots k_{l-1}} - \sum_{i=1}^{p} u^\lambda{}_{k_1 \cdots k_{l-1} i} \cdot \omega^i, \\
&\qquad (\lambda = 1, \cdots, m; k_1, \cdots, k_{l-1} = 1, \cdots, p; \nu = 1, \cdots, l-1).
\end{aligned}
$$

We shall consider $*\varpi^\lambda$ as the case $\nu=0$ of $*\varpi^\lambda_{k_1\cdots k_\nu}$. It is obvious that $\omega^1,\cdots,\omega^p$, the elements of (Π_l), and $du_{k_1\cdots k_l}$ form a base of Pfaffian forms on $\mathfrak{R}_l$. Thus

$$\dim\langle\Pi_l,\mathcal{E}_y\mathfrak{R}_l\rangle+p=\sum_{\nu=0}^{l-1}n_\nu=\dim\mathfrak{R}_{l-1} \tag{20}$$

for any y in $\mathfrak{R}_l$. If f is a function on $\mathfrak{R}_{l-1}$, $d(f\circ\rho_{l-1}{}^l)$ is in $(\rho_{l-1}{}^l)^*\Lambda^1\mathfrak{R}_{l-1}$. Therefore, for any function f on $\mathfrak{R}_{l-1}$, we can define the function $D_k{}^l\cdot f$, $(k=1,\cdots,p)$, on $\mathfrak{R}_l$ by the formula:

$$d(f\circ\rho_{l-1}{}^l)\doteq\sum_{k=1}^{p}(D_k{}^l\cdot f)\cdot\omega^k\ (\mathrm{mod}\,\Pi_l). \tag{21}$$

It is easy to see that, if $l_1\geqq l$, $D_k{}^{l_1}(f\circ\rho_{l-1}{}^{l_1-1})=(D_k{}^l\cdot f)\circ\rho_l{}^{l_1}$. Hence we may omit the index l and simply write $D_k\cdot f$. Let D_k be the mapping of the vector space of analytic functions on $\mathfrak{R}_{l-1}$ to that on $\mathfrak{R}_l$ of which value at f is $D_k\cdot f$. Since $d(d(f\circ\rho_{l-1}{}^l)=0$,

$$D_k\circ D_h=D_h\circ D_k,\qquad (h,k=1,\cdots,p). \tag{22}$$

Clearly, they have the usual properties of differentiation. For example,

$$D_k\cdot(f\cdot g)=(D_k\cdot f)\cdot g+f\cdot(D_k\cdot g). \tag{23}$$

By the condition (ii) of the normal system, we can write, for any ϕ in $\Sigma^{[2]}$,

$$\phi\equiv\sum_{i=1}^{p}\sum_{\lambda=1}^{m}A_{\phi;i\lambda}\omega^i\wedge\varpi^\lambda+\sum_{i=1}^{p}\sum_{j=1}^{p}\tfrac{1}{2}B_{\phi;ij}\omega^i\wedge\omega^j\quad(\mathrm{mod}\,\Sigma^1) \tag{24}$$

where $A_{\phi;i\alpha}$ and $B_{\phi;ij}$ are analytic functions on $\mathfrak{V}$ and $B_{\phi;ij}+B_{\phi;ji}=0$. Set

$$\Theta_{\phi;ij;}=\sum_{\lambda=1}^{m}(A_{\phi;i\lambda}\cdot u_j{}^\lambda-A_{\phi;j\lambda}\cdot u_i{}^\lambda)+B_{\phi;ij}. \tag{25}$$

They are analytic functions on $\mathfrak{R}_l$ for $l\geqq 1$. Starting from $\Theta_{\phi;ij;}$, we shall define analytic functions $\Theta_{\phi;ij;k_1\cdots k_{l-1}}$ $(i,j,k_1,\cdots,k_{l-1}=1,\cdots,p)$ on $\mathfrak{R}_{l'}$ $(l'\geqq l)$, by the formula:

$$\Theta_{\phi;ij;k_1\cdots k_{l-1}}=D_{k_{l-1}}\circ\cdots\circ D_{k_2}\circ D_{k_1}(\Theta_{\phi;ij;}). \tag{26}$$

For simplicity, we shall denote by $\mathcal{K}_l$ the set $k_1,\cdots,k_l$. $\mathcal{K}_lk$, $k\mathcal{K}_l$ means the set $k_1\cdots k_lk$, $kk_1\cdots k_l$, respectively.

By (22), $\Theta_{\phi;ij;\mathcal{K}_{l-1}}$ are symmetric with respect to the indexes $k_1,\cdots,k_{l-1}$, and it is easy to see, by induction on l, that

$$\Theta_{\phi;i,j;\mathcal{K}_{l-1}}=\sum_{\lambda=1}^{m}(A_{\phi;i\lambda}u^\lambda{}_{j\mathcal{K}_{l-1}}-A_{\phi;j\lambda}u^\lambda{}_{i\mathcal{K}_{l-1}})+B_{\phi;ij;\mathcal{K}_{l-1}} \tag{27}$$

where $B_{\phi;ij;\varkappa_{l-1}}$ are analytic functions on $\mathfrak{R}_{l_1}$ for $l_1 \geqq l-1$. Therefore it follows that $B_{\phi;ij;\varkappa_{l-1}}$ are symmetric with respect to the indexes $k_1, \cdots, k_{l-1}$. $B_{\phi;ij;\varkappa_{l-1}}$ are defined inductively by the formula:

$$(28) \quad B_{\phi;ij;k_1\cdots k_{l-1}} = \sum_{\lambda=1}^{m} \{ (D_{k_{l-1}} \cdot A_{\phi;i\lambda}) \cdot u^{\lambda}{}_{jk_1\cdots k_{l-2}} - (D_{k_{l-1}} \cdot A_{\phi;j\lambda}) \cdot u^{\lambda}{}_{ik_1\cdots k_{l-2}} \} + D_{k_{l-1}} \cdot B_{\phi;ij;k_1\cdots k_{l-2}},$$

$(l \geqq 2)$, where, when $l-1=0$, $B_{\phi;ij;k_1\cdots k_{l-1}}$ means $B_{\phi;ij}$.

Let $\mathfrak{R}_l{}^{[0]}\Sigma$ be the ideal of $\Lambda^0\mathfrak{R}_l$ generated by all $\Theta_{\phi;ij;\varkappa_\nu}$ $(i, j, k_1, \cdots, k_\nu = 1, \cdots, p;\ \nu = 0, 1, \cdots, l-1;\ \phi \in \Sigma^{[2]})$. Since $\Sigma^{[2]}$ is finitely generated, $\mathfrak{R}_l{}^{[0]}\Sigma$ is also finitely generated.

Definition II. 2. Let $\mathfrak{R}_l\Sigma$ be the exterior differential system on $\mathfrak{R}_l$ generated by Π_l and $\mathfrak{R}_l{}^{[0]}\Sigma$, for $l \geqq 1$.

Set $\mathfrak{R}_0\Sigma = \Sigma$ on $\mathfrak{V}$. It is easy to prove the following relations:

$$(29)_l \qquad \text{if } 0 \leqq \nu \leqq l-2, \quad d\Theta_{\phi;ij;\varkappa_\nu} \equiv \sum_{k=1}^{p} \Theta_{\phi;ij;\varkappa_\nu k}\,\omega^k \quad (\text{mod. } \pi_l),$$

$$(30)_l \qquad d\Theta_{\phi;ij;\varkappa_{l-1}} \equiv \sum_{\lambda=1}^{m} (A_{\phi;i\lambda}\, du^{\lambda}{}_{j\varkappa_{l-1}} - A_{\phi;j\lambda} du^{\lambda}{}_{i\varkappa_{l-1}}) + \sum_{k=1}^{p} B_{\phi;ij;\varkappa_{l-1}k},$$

$$(31)_l \qquad d\theta^{\alpha} \equiv 0 \quad \text{mod}\{\Theta_{\phi;ij;};\ \phi \in \Sigma^{[2]}, i, j = 1, \cdots, p\},$$

$$(32)_l \qquad d^*\varpi^{\lambda}{}_{\varkappa_\nu} = \sum_{k=1}^{p} {}^*\varpi^{\lambda}{}_{\varkappa_\nu k} \wedge \omega^k.$$

THEOREM II. 2. $(\mathfrak{R}_l\Sigma, \Omega)$ *on* $\mathfrak{R}_l$ *is isomorphic to an admissible restriction of* $\mathfrak{P}^l(\Sigma, \Omega)$ $(l = 0, 1, \cdots)$. *The character* c_l *of the restriction is equal to* $\sum_{\nu=0}^{l-1} (p+1)^{l-1-\nu} c_\nu'$, *where* $c_0' = \alpha_1 p$ *and*

$$c_\nu' = \alpha_1 p + \tfrac{1}{2} mp(p-1)(C_{\nu-1}{}^{p+\nu-2}) + \sum_{h=1}^{\nu-1} (C_h{}^{p+h-1}) \quad \text{for } \nu \geqq 1.$$

Proof. (Induction on l). In the case $l=0$, the theorem is trivial. Assuming that the theorem holds for l, we shall prove it for $l+1$. The proof for the case $l+1=1$ is almost the same as that for the case $l+1>1$ and is easier. Therefore we shall deal with the case $l+1>1$. By Propositions II. 2 and II. 3, it is sufficient to show that $(\mathfrak{R}_{l+1}\Sigma, \Omega)$ is isomorphic to an admissible restriction of $\mathfrak{P}(\mathfrak{R}_l\Sigma, \Omega)$ of the character c_l'.

$\omega^1, \cdots, \omega^p$, $(\Pi_l), \cdots, du^{\lambda}{}_{k_1\cdots k_l}$ form a base of Pfaffian forms on $\mathfrak{R}_l$. Hence as in **4** of Preliminaries, $\mathfrak{G}_\Omega(\mathfrak{R}_l, p) = \mathfrak{G}(\mathfrak{R}_l, p)$ has a system of coordinates $x^1, \cdots, x^n, \cdots, u^{\lambda}{}_{k_1\cdots k_\nu}, \cdots$, $(\nu = 1, \cdots, l)$,

$$v_k{}^{\alpha}, v^{\lambda}{}_{;k}, \cdots, v^{\lambda}{}_{\varkappa_\nu;k}, \cdots, v^{\lambda}{}_{\varkappa_{l-1};k}, w^{\lambda}{}_{\varkappa_l;k}$$

defined as follows: (i) $x^1, \cdots, x^n$ is a system of coordinates on $\mathfrak{V}$, (ii) if E is in $\mathfrak{G}(\mathfrak{R}_l, p)$, E is the space of all solutions of the following system of linear equations on the tangent vector space to $\mathfrak{R}_l$ at the origin of E:

$$
\begin{gathered}
\theta^\alpha - \sum_{k=1}^{p} v_k{}^\alpha(E)\omega^k = 0, \\
*\varpi^\lambda - \sum_{k=1}^{p} v^\lambda{}_{;k}(E)\omega^k = 0, \qquad *\varpi^\lambda{}_{k_1} - \sum_{k=1}^{p} v^\lambda{}_{k_1;k}(E)\omega^k = 0, \cdots, \\
*\varpi^\lambda{}_{\boldsymbol{\varkappa}_{l-1}} - \sum_{k=1}^{p} v^\lambda{}_{\boldsymbol{\varkappa}_{l-1};k}(E)\omega^k = 0, \qquad du^\lambda{}_{\boldsymbol{\varkappa}_l} - \sum_{k=1}^{p} w^\lambda{}_{\boldsymbol{\varkappa}_l;k}(E)\omega^k = 0.
\end{gathered} \tag{33}
$$

To avoid confusion, let Ω_l be the system of independent variables Ω on $\mathfrak{R}_l$ and ρ_l be the projection $\mathfrak{G}(\mathfrak{R}_l, p) \to \mathfrak{R}_l$. Then, by Proposition I. 8, $\Pi^{[1]}\Omega_l$ is generated by

$$
\begin{gathered}
\theta^\alpha - \sum_{k=1}^{p} v_k{}^\alpha\omega^k, \qquad *\varpi^\lambda - \sum_{k=1}^{p} v^\lambda{}_{;k}\omega^k, \qquad *\varpi^\lambda{}_{k_1} - \sum_{k=1}^{p} v^\lambda{}_{k_1;k}\omega^k, \cdots, \\
*\varpi^\lambda{}_{\boldsymbol{\varkappa}_{l-1}} - \sum_{k=1}^{p} v^\lambda{}_{\boldsymbol{\varkappa}_{l-1};k}\omega^k, \qquad du^\lambda{}_{\boldsymbol{\varkappa}_l} - \sum_{k=1}^{p} w^\lambda{}_{\boldsymbol{\varkappa}_l;k}\omega^k.
\end{gathered} \tag{34}
$$

Then, by Definition I. 19 and Lemma I. 2, it follows that $(\mathfrak{P}\mathfrak{R}_l\Sigma)^{[0]}$ is generated by

$$\Theta_{\phi;ij;\boldsymbol{\varkappa}_\nu}, \quad (\nu = 0, 1, \cdots, l-1; \phi \in \Sigma^{[2]}),$$

$$K[d\Theta_{\phi;ij;\boldsymbol{\varkappa}_\nu}, p; k] \equiv \Theta_{\phi;ij;\boldsymbol{\varkappa}_\nu k}, \bmod (v^\lambda{}_{;k}, v^\lambda{}_{j_1;k}, \cdots, v^\lambda{}_{j_1\cdots j_{l-1};k}), \text{ (cf. } (29)_l),$$

$$
\begin{aligned}
K[d\Theta_{\phi;ij;\boldsymbol{\varkappa}_{l-1}}, p; k] \equiv \sum_{\lambda=1}^{m} (A_{\phi;i\lambda} w^\lambda{}_{j\boldsymbol{\varkappa}_{l-1};k} \\
- A_{\phi;j\lambda} w^\lambda{}_{i\boldsymbol{\varkappa}_{l-1};k}) + B_{\phi;ij;\boldsymbol{\varkappa}_{l-1}}, \bmod (v^\lambda{}_{;k}, v^\lambda{}_{j_1;k}, \cdots, v^\lambda{}_{j_1\cdots j_{l-1};k}), \text{ (cf. } (30)_l),
\end{aligned}
$$

$$
\begin{aligned}
&K_k{}^{\theta^\alpha} = v_k{}^\alpha, \; K[*\varpi^\lambda, p; k] = v^\lambda{}_{;k}, \\
&\qquad K[*\varpi^\lambda{}_{k_1}, p; k] = v^\lambda{}_{k_1;k}, \cdots, \; K[*\varpi^\lambda{}_{\boldsymbol{\varkappa}_{l-1}}, p; k] = v_{\boldsymbol{\varkappa}_{l-1};k} \\
&K[d*\varpi^\lambda{}_{\boldsymbol{\varkappa}_\nu}, p; i, j] \equiv 0 \; (\bmod v^\lambda{}_{;k}, v^\lambda{}_{j_1;k}, \cdots, v^\lambda{}_{j_1\cdots j_{l-1};k}), \\
&\qquad\qquad (\nu = 0, 1, \cdots, l-2; \text{ cf. } (32)_l), \\
&K[d*\varpi^\lambda{}_{\boldsymbol{\varkappa}_{l-1}}, p; i, j] = w^\lambda{}_{\boldsymbol{\varkappa}_{l-1}i;j} - w^\lambda{}_{\boldsymbol{\varkappa}_{l-1}j;i}, \text{ and} \\
&\qquad K[d\theta^\alpha, p; i, j] \equiv 0 \quad (\bmod \Theta_{\phi;k_1k_2}).
\end{aligned}
$$

Let Σ^* be the restriction of $\mathfrak{P}_\Omega\mathfrak{R}_l\Sigma$ to the submanifold $\mathfrak{G}^*$ of $\mathfrak{G}(\mathfrak{R}_l, p)$ defined by the equations:

$$
\begin{gathered}
v_k{}^\alpha = v^\lambda{}_{;k} = v^\lambda{}_{k_1;k} = \cdots = v^\lambda{}_{\boldsymbol{\varkappa}_{l-1};k} = w^\lambda{}_{\boldsymbol{\varkappa}_{l-1}i;j} - w^\lambda{}_{\boldsymbol{\varkappa}_{l-1}j;i} = 0 \\
(\alpha = 1, \cdots, \alpha_1; \lambda = 1, \cdots, m; i, j, k, k_1, \cdots, k_{l-1} = 1, \cdots, p).
\end{gathered} \tag{35}
$$

Then Σ^* is an admissible restriction of $\mathcal{P}_\Omega\mathcal{R}_l\Sigma$ of character c_l' and $\Sigma^{*[0]}$ is generated by all $\Theta_{\phi;ij;}, \Theta_{\phi;ij;k_1}, \cdots, \Theta_{\phi;ij;\varkappa_{l-1}}$, and by

$$\sum_{\lambda=1}^{m} (A_{\phi;i\lambda}w^\lambda{}_{j\varkappa_{l-1};k} - A_{\phi;j\lambda}w^\lambda{}_{i\varkappa_{l-1};k}) + B_{\phi;ij;\varkappa_{l-1}k}.$$

$\Sigma^{*[1]}$ is generated by $d\Sigma^{*[0]}$, by θ^α, $*\varpi^\lambda$, $*\varpi^\lambda{}_{k_1},\cdots, *\varpi_{\varkappa_{l-1}}$, and by $du^\lambda{}_{\varkappa_{l-1}} - \sum_{k=1}^{p} w^\lambda{}_{\varkappa_{l-1};k}\omega^k$. Σ^* is generated by $\Sigma^{*[0]}$, $\Sigma^{*[1]}$, and $d\Sigma^{[1]}$. Then it is clear that the mapping $\mathcal{R}_{l+1} \to \mathcal{G}^*$, defined by $u^\lambda{}_{k_1\cdots k_{l+1}} \to w^\lambda{}_{k_1\cdots k_l;k_{l+1}}$ and by $\mathcal{R}_l \to \mathcal{R}_l$ (identity mapping), is well defined and induces an isomorphism from $(\mathcal{R}_{l+1}\Sigma, \Omega)$ onto $(\mathcal{G}^*, \Omega)$. The number of independent equations in (35) is equal to c_l'. Thus the proof of Theorem II.2 is completed.

4. System of polar forms of $\mathcal{R}_l\Sigma$. Let us make explicit the system of polar forms $J(E)$ of an integral element E of $(\mathcal{R}_l\Sigma, \Omega)$. Let ρ_q be the projection of $\mathcal{G}(\mathcal{R}_l, q) = \mathcal{G}_\Omega(\mathcal{R}_l, q)$ onto $\mathcal{R}_l$. We shall omit $\circ\rho_q$ and ρ_q^* in $A_{\phi;i\lambda}\circ\rho_q$, $\rho_q^*\omega^i$, etc., since the omission will not cause any confusion. Note that $\omega^1, \cdots, \omega^p, \theta^1, \cdots, \theta^{\alpha_1}, \varpi^1, \cdots, \varpi^m$ is the base of Pfaffian forms on $\mathcal{V}$ fixed at the beginning of § 3.

(36) $\mathcal{V}_l{}^q = \{E \in \mathcal{G}(\mathcal{R}_l, q)\,;\ \omega^1, \cdots, \omega^q$ are linearly independent on $E\}$.

$\mathcal{V}_l{}^q$ is an open submanifold of $\mathcal{G}(\mathcal{R}_l, q)$ and $\mathcal{V}_l{}^p = \mathcal{G}(\mathcal{R}_l, p)$. Define the tangent vectors $L_1(E), \cdots, L_q(E)$ to $\mathcal{R}_l$, contained in E, by the formulas:

(37) $$\langle\omega^{r'}, L_r(E)\rangle = \delta_r{}^{r'} \qquad (r', r = 1, \cdots, q),$$

for any E in $\mathcal{V}_l{}^q$. Denote by η_q the projection of $\mathcal{V}_l{}^q$ onto $\mathcal{V}_l{}^{q-1}$ defined by the formula

(38) $$\eta_q(E) = \{\text{the space spanned by } L_1(E), \cdots, L_{q-1}(E)\},$$

$(E \in \mathcal{V}_l{}^q)$. η_q is defined for $q = 1, \cdots, p$. Define analytic functions $w_r{}^{q,h}$ and $w^{q,\lambda}{}_{\varkappa_l;r}$ on $\mathcal{V}_l{}^q$ by the formula:

(39) $$w_r{}^{q,h}(E) = \langle\omega^{q+h}, L_r(E)\rangle, \qquad w^{q,\lambda}{}_{\varkappa_l;r}(E) = \langle du^\lambda{}_{\varkappa_l}, L_r(E)\rangle,$$

$(E \in \mathcal{V}_q{}^l\,;\ r = 1, \cdots, q\,;\ h = 1, \cdots, p-q\,;\ \lambda = 1, \cdots, m\,;\ k_1 \cdots k_l = 1, \cdots, p)$.

Clearly we have

(40) $$w_r{}^{q-1,h+1}\circ\eta_q = w_r{}^{q,h}, \qquad (41) \quad w^{q-1,\lambda}{}_{\varkappa_l;r}\circ\eta_q = w^{q,\lambda}{}_{\varkappa_l;r},$$

for $r = 1, \cdots, q-1$. Denote by $\rho_q^*\cdot\Lambda^1\mathcal{R}_l$ the $\Lambda^0\mathcal{V}_l{}^q$-submodule of $\Lambda^1\mathcal{V}_l{}^q$ generated by all $\rho_q^*\cdot\theta, \theta \in \Lambda^1\mathcal{R}_l$.

Definition II. 3. Denote by $\boldsymbol{A}_l{}^q$ the $\Lambda^0\mathfrak{V}_l{}^q$-submodule of $\rho_q{}^*\cdot\Lambda^1\mathfrak{R}_l$ generated by the following set of Pfaffian forms defined on $\mathfrak{V}_q{}^l$:

$$\xi_{\phi\,;ij\,;\varkappa_{l-1}} = \sum_{\lambda=1}^{m}(A_{\phi\,;i\lambda}du^\lambda{}_{j\varkappa_{l-1}} - A_{\phi\,;j\lambda}du^\lambda{}_{i\varkappa_{l-1}}) + \sum_{k=1}^{p} B_{\phi\,;ij\,;\varkappa_{l-1}k}\omega^k,$$

$$(\boldsymbol{A}_l{}^q) \qquad \zeta^\lambda{}_{\varkappa_{l-1};r} = du^\lambda{}_{\varkappa_{l-1}r} + \sum_{h=1}^{p-q} w_r{}^{q,h}\, du^\lambda{}_{\varkappa_{l-1}q+h} - \sum_{k=1}^{p} w^{q,\lambda}{}_{\varkappa_{l-1}k\,;r}\cdot\omega^k$$

$$(\phi\in\Sigma^{[2]};\ i,j,k_1,\cdots,k_{l-1}=1,\cdots,p;\ \lambda=1,\cdots,m;\ r=1,\cdots,q).$$

We remark that $\boldsymbol{A}_l{}^0$ is the submodule generated by all $\xi_{\phi\,;ij\,;\varkappa_{l-1}}$. According to the notations in § **5** of Chapter I, if

$$\xi = f_1\cdot\rho_q{}^*\theta_1 + \cdots + f_a\cdot\rho_q{}^*\theta_a,$$
$$(f_1,\cdots,f_a\in\Lambda^0\mathfrak{V}_l{}^q,\ \theta_1,\cdots,\theta_a\in\Lambda^1\mathfrak{R}_l),$$

and if E is in $\mathfrak{V}_l{}^q$, then $\langle\xi,\mathcal{E}_y\mathfrak{R}_l\rangle_E$, where y is the origin of E, is the linear functional on the tangent vector space $\mathcal{E}_y\mathfrak{R}_l$ to $\mathfrak{R}_l$ at y, defined by the formula: $\langle\xi,\mathcal{E}_y\mathfrak{R}_l\rangle_E = f_1(E)\cdot\langle\theta_1,\mathcal{E}_y\mathfrak{R}_l\rangle + \cdots + f_a(E)\cdot\langle\theta_a,\mathcal{E}_y\mathfrak{R}_l\rangle$. Then we have the following

Proposition II. 4. If E is in $\mathfrak{V}_q{}^l$ and if the origin $y=\rho_q(E)$ is an integral point of $\mathfrak{R}_l\Sigma$, then

$$J(E) = \langle\pi_l,\mathcal{E}_y\mathfrak{R}_l\rangle + \langle\boldsymbol{A}_l{}^q,\mathcal{E}_y\mathfrak{R}_l\rangle_E,$$

where the plus sign denotes the direct sum.

Proof. By the definition of $J(E)$, (Definition I. 6), it is generated by the following linear functionals on $\mathcal{E}_y\mathfrak{R}_l$:

$$(42)_\nu \qquad \langle d\Theta_{\phi\,;ij\,;\varkappa_\nu},\mathcal{E}_y\mathfrak{R}_l\rangle$$

for $\nu=0,1,\cdots,l-1$,

$$(43) \qquad \langle\Pi_l,\mathcal{E}_y\mathfrak{R}_l\rangle,$$

$$(44) \qquad d\theta^a[L_r(E)],\ \text{and}\ d^*\varpi^\lambda{}_{\varkappa_\nu}[L_r(E)], \qquad (\nu=0,1,\cdots,l-1).$$

(cf. (10)). Since y is an integral point of $\mathfrak{R}_l\Sigma$, $(29)_l$ implies that the members in $(42)_\nu$ are congruent to 0 modulo (43) for $\nu=0,1,\cdots,l-2$. $(30)_l$ implies that

$$\langle d\Theta_{\phi\,;ij\,;\varkappa_{l-1}},\mathcal{E}_y\mathfrak{R}_l\rangle \equiv \langle\xi_{\phi\,;ij\,;\varkappa_{l-1}},\mathcal{E}_y\mathfrak{R}_l\rangle_E$$

modulo $\langle\pi_l,\mathcal{E}_y\mathfrak{R}_l\rangle$. By $(31)_l$ and $(32)_l$, members in (44) are congruent to 0 modulo (43) except $d^*\varpi^\lambda{}_{k_1\cdots k_{l-1}}[L_r(E)]$. A direct calculation shows that

$$-d^*\varpi^\lambda{}_{\varkappa_{l-1}}[L_r(E)] = \langle\zeta^\lambda{}_{\varkappa_{l-1};r},\mathcal{E}_y\mathfrak{R}_l\rangle_E.$$

Hence $J(E)$ is generated by $\langle\Pi_l, \mathcal{E}_y\mathcal{R}_l\rangle$ and $\langle A_l^q, \mathcal{E}_y\mathcal{R}_l\rangle_E$. Since ${}^*\varpi^\lambda{}_{\mathcal{K}_\nu}$ $(\nu=0,1,\cdots,l-1)$, $\omega^1,\cdots,\omega^p$, $du_{\mathcal{K}_l}$ form a base of Pfaffian forms on $\mathcal{R}_l$, we see easily, by the explicit expressions for the members in (Π_l) and (A_l^q), that the summation must be a direct sum.

Proposition II. 5. Let $A_l(q)$, $p\geqq q\geqq 1$, be the $\Lambda^0\mathcal{V}_l^q$-submodule of $\rho_q{}^*\Lambda^1\mathcal{R}_l$ generated by all $\zeta^\lambda{}_{k_1\cdots k_{l-1};q}$. Let E be an element in $\mathcal{V}_l^q$ whose origin y is an integral point of $\mathcal{R}_l\Sigma$. Set $E'=\eta_q(E)$. Then $\langle A_l^q, \mathcal{E}_y\mathcal{R}_l\rangle_E$ is generated by $\langle A_l^{i-1}, \mathcal{E}_y\mathcal{R}_l\rangle_{E'}$ and $\langle A_l(q), \mathcal{E}_y\mathcal{R}_l\rangle_E$.

Proof. Clearly $L_r(E')=L_r(E)$ for $r=1,\cdots,q-1$. Then the proposition follows from the definition of A_l^q, (40), and from (41).

In the following, we shall write $\mathcal{K}$ instead of $\mathcal{K}_{l-1}$.

Definition II. 4. Denote by $A'_l{}^q$ the $\Lambda^0\mathcal{V}_l^q$-submodule of $\rho_q{}^*\cdot\Lambda^1\mathcal{R}_l$ generated by the following set of Pfaffian forms defined on $\mathcal{V}_l^q$.

$$(A'_l{}^q)\qquad \begin{aligned} \xi'_{\phi;ij;\mathcal{K}} &= \sum_{\lambda=1}^{m}(A_{\phi;i\lambda}du^\lambda{}_{j\mathcal{K}} - A_{\phi;j\lambda}du^\lambda{}_{i\mathcal{K}}),\\ \zeta'^\lambda{}_{\mathcal{K};r} &= du_{\mathcal{K}r} + \sum_{h=1}^{p-q} w_r{}^{q,h}du_{\mathcal{K}\,q+h},\end{aligned}$$

$$(\phi\in\Sigma^{[2]};\ \lambda=1,\cdots,m;\ r=1,\cdots,q;\ i,j,k_1,\cdots,k_{l-1}=1,\cdots,p).$$

Set

$$(45)\qquad t'(E)=\dim\langle A'_l{}^q, \mathcal{E}_y\mathcal{R}_l\rangle_E,\qquad (y=\text{the origin of } E, E\in\mathcal{V}_l^q).$$

Then by Proposition II. 4 we have the formula

$$(45)'\quad \dim(J(E) \bmod \langle\Omega, \mathcal{E}_y\mathcal{R}_l\rangle) = t'(E)+n-p+m\Big(\sum_{\nu=1}^{l-1}C_\nu{}^{p+\nu-1}\Big).$$

Proposition II. 6. Let E be a q-dimensional integral element of $\mathcal{R}_l\Sigma$. Assume that E is $\mathcal{V}_l^q$. Set $E'=\eta_q(E)$ (cf. (38)), and $E''=d\rho_{l-1}{}^l\cdot E'$, where $\rho_{l-1}{}^l$ is the projection $\mathcal{R}_l\to\mathcal{R}_{l-1}$. Let y be the origin of E. Then

$$t'(E)\leqq\dim\langle A_l^q, \mathcal{E}_y\mathcal{R}_l\rangle_E\leqq\dim\langle A_l^{q-1}, \mathcal{E}_y\mathcal{R}_l\rangle_{E'}+n_{l-1}-t'(E''),$$

where $n_{l-1}=\dim\mathcal{R}_{l-1}=m\cdot C_{l-1}{}^{p+l-2}$.

To simplify the notations we shall omit $\langle\ ,\mathcal{E}_y\mathcal{R}_l\rangle$ and $\langle\ ,\mathcal{E}_y\mathcal{R}_l\rangle_E$. Thus, for example, $du^\lambda{}_{\mathcal{K}}$ and $\zeta^\lambda{}_{\mathcal{K};r}$ means $\langle du^\lambda{}_{\mathcal{K}}, \mathcal{E}_y\mathcal{R}_l\rangle$ and $\langle\zeta^\lambda{}_{\mathcal{K};r}, \mathcal{E}_y\mathcal{R}_l\rangle_E$, respectively. In general, we shall denote by $\mathcal{H}$ the set of indexes $k_1,\cdots,k_{l-2}$. As before, $\mathcal{K}$ represents the set of indexes $k_1,\cdots,k_{l-1}$. Let $du_{\mathcal{K}_\chi}{}^{\lambda_\chi}$, $(\chi\in\mathrm{X})$, be the maximal number independent $du_{\mathcal{K}}{}^\lambda \bmod \langle A'_{l-1}{}^{q-1}, \mathcal{E}_{y'}\mathcal{R}_{l-1}\rangle_{E''}\circ d\rho_{l-1}{}^l$, where $y'=\rho_{l-1}{}^l(y)$ and X is a set of indexes. Then the number of elements

in X is $n_{l-1}-t'(E'')$. Take any λ and $\mathfrak{K}$. Then, adopting the tensor notations, we can write

$$du^{\lambda}{}_{\mathfrak{K}}=a_{\chi}du^{\lambda\chi}{}_{\mathfrak{K}_{\chi}}+b^{\phi;ij;\mathfrak{A}}\xi'_{\phi;ij;\mathfrak{A}}\circ d\rho^{l}{}_{l-1}+c_{\lambda}{}^{\mathfrak{A};r'}\zeta'^{\lambda}{}_{\mathfrak{A};r'}\circ d\rho^{l}{}_{l-1},$$

$(r'=1,\cdots,q-1)$, where a_{χ}, $b^{\phi;ij;\mathfrak{A}}$, $c_{\lambda}{}^{\mathfrak{A};r'}$ are constants. We claim that, for any $k=1,\cdots,p$,

$$\text{(a)}\qquad du^{\lambda}{}_{\mathfrak{K}k}=a_{\chi}du^{\lambda\chi}{}_{\mathfrak{K}_{\chi}k}+b^{\phi;ij;\mathfrak{A}}\xi'_{\phi;ij;\mathfrak{A}k}+c_{\lambda}{}^{\mathfrak{A};r'}\zeta'_{\mathfrak{A}k;r'}.$$

To prove formula (a), observe that, for each k, there is an isomorphism of the space generated by $\langle du^{\lambda}{}_{\mathfrak{A}},\mathcal{E}_{y'}(\mathcal{R}^{l-1})\rangle$ which maps each $du^{\lambda}{}_{\mathfrak{A}}$ upon $du^{\lambda}{}_{\mathfrak{A}k}$. Then clearly this mapping maps $\xi'_{\phi;ij;\mathfrak{A}}$ upon $\xi'_{\phi;ij;\mathfrak{A}k}$. Since $w_{r}{}^{q,h}(E)=w_{r}{}^{q,h}(\rho^{l}{}_{l-1}(E))$ by (39), it follows that this mapping maps $\zeta'^{\lambda}{}_{\mathfrak{A};r'}$ upon $\zeta'^{\lambda}{}_{\mathfrak{A}k;r'}$. Therefore formula (a) holds.

Since E is an integral element of $\mathcal{R}_{l}\Sigma$, taking the value at $L_{q}(E)$, we have the equality

$$\begin{aligned}\text{(b)}\quad w^{q,\lambda}{}_{\mathfrak{K}k;q}(E)&=a_{\chi}w^{q,\lambda\chi}{}_{\mathfrak{K}_{\chi}k;q}(E)-b^{\phi;ij;\mathfrak{A}}(B_{\phi;ij;\mathfrak{A}kq}(y)\\&\quad+w_{q}{}^{q,h}(E)B_{\phi;ij;\mathfrak{A}kq+h}(y))+c_{\lambda}{}^{\mathfrak{A};r'}(w^{q,\lambda}{}_{\mathfrak{A}kq;r'}(E)\\&\quad+w_{q}{}^{q,h}(E)w^{q,\lambda}{}_{\mathfrak{A}kq+h;r'}(E)).\end{aligned}$$

Then, by (a) and (b),

$$\begin{aligned}\zeta^{\lambda}{}_{\mathfrak{K};q}&=du^{\lambda}{}_{\mathfrak{K}q}+w_{q}{}^{q,h}(E)du^{\lambda}{}_{\mathfrak{K}q+h}-w^{q,\lambda}{}_{\mathfrak{K}k;q}(E)\omega^{k}\\&=a_{\chi}\zeta^{\lambda\chi}{}_{\mathfrak{K}_{\chi};q}+b^{\phi;ij;\mathfrak{A}}(\xi_{\phi;ij;\mathfrak{A}q}+w_{q}{}^{q,h}(E)\xi_{\phi;ij;\mathfrak{A}q+h})\\&\quad+c_{\lambda}{}^{\mathfrak{A};r'}(\zeta^{\lambda}{}_{\mathfrak{A}q;r'}+w_{q}{}^{q,h}(E)\xi^{\lambda}{}_{\mathfrak{A}q+h;r'}),\end{aligned}$$

since $B_{\phi;ij;k_1\cdots k_l}$ and $w^{q,\lambda}{}_{k_1\cdots k_l;r}$ are symmetric with respect to the indexes $k_1,\cdots,k_l$. Therefore

$$\zeta^{\lambda}{}_{\mathfrak{K};q}\equiv a_{\chi}\zeta^{\lambda\chi}{}_{\mathfrak{K}_{\chi};q}\ (\mathrm{mod}\ \langle A_{l}{}^{q-1},\mathcal{E}_{y}\mathcal{R}_{l}\rangle_{E'}\circ d\rho^{l}{}_{l-1}).$$

Then, by Proposition II. 5,

$$\begin{aligned}\dim\langle A_{l}{}^{q},\mathcal{E}_{y}\mathcal{R}_{l}\rangle_{E}&\leqq\dim\langle A_{l}{}^{q-1},\mathcal{E}_{y}\mathcal{R}_{l}\rangle_{E'}+\text{the number of indexes in X}\\&=\dim\langle A_{l}{}^{q-1},\mathcal{E}_{y}\mathcal{R}_{l}\rangle_{E'}+n_{l-1}-t'(E'').\end{aligned}$$

Chapter III. Prolongation Theorem.

The problem we are going to concern ourselves with is the following: when the given normal system (Σ, Ω) is not involutive (Definition I. 17), what are the conditions that will assure the involutiveness of the l-th prolongation $\mathcal{P}^l(\Sigma, \Omega)$ of (Σ, Ω) for sufficiently large l? By Theorem II. 2, it is sufficient, for that purpose, to examine $(\mathcal{R}_l\Sigma, \Omega)$. We shall first study the ranks of the reduced polar equations of integral elements, which are equal to the dimensions of the $A'_l{}^q$. The Definition II. 4 suggests that they may be equal to the dimensions of homogeneous parts of appropriately defined ideals in some polynomial rings. This will be done in § **1** and § **2**. Then, using the Noetherian property of polynomial ring, we shall derive, in § **3**, the crucial property of the reduced characters, which will help, with Proposition II. 6, to bridge the characters and the reduced characters (§ **5**). To complete this bridge, we must choose points which are regular in some respects (§ **4**), and the differential system must satisfy some conditions. The exact form of the conditions will be given in the fundamental theorem in § **6**. These conditions are also necessary for $\mathcal{P}^l(\Sigma, \Omega)$ to be involutive. In § 7, we shall give an example which indicates that our conditions are, in some respect, the best possible one.

1. Fiber bundles associated with a system of independent variables. Let Ω be a system of p independent variables on $\mathcal{V}$. For any point x of $\mathcal{V}$, denote by $\mathcal{E}^*_x\mathcal{V}$ the space of all tangent vectors L to $\mathcal{V}$ at x such that $\langle \omega, L \rangle = 0$ for all $\omega \in \Omega$. Set $\mathcal{E}^\dagger_x\mathcal{V} = \mathcal{E}_x\mathcal{V}/\mathcal{E}^*_x\mathcal{V}$. It is a p-dimensional space. The elements in $\mathcal{E}^\dagger_x\mathcal{V}$ will be called a reduced tangent vector to $\mathcal{V}$ at x (with respect to Ω). It is clear that $\mathcal{E}^\dagger\mathcal{V} = \bigcup \{\mathcal{E}^\dagger_x\mathcal{V}; x \in \mathcal{V}\}$ has a natural analytic manifold structure and is a fiber bundle over $\mathcal{V}$ with fiber $\mathcal{E}^\dagger_x\mathcal{V}$. Denote by $\rho^\dagger$ the projection. A q dimensional subspace $E^\dagger$ of $\mathcal{E}^\dagger_x\mathcal{V}$ will be called a reduced contact element to $\mathcal{V}$ at x (with respect to Ω), and x its origin. If $\omega \in \Omega$, we can naturally define $\langle \omega, E^\dagger \rangle$ as a linear functional on $E^\dagger$. The set of all q dimensional reduced contact elements forms an analytic manifold $\mathcal{G}^\dagger(\mathcal{V}, q)$. It is a fiber bundle with the base manifold $\mathcal{V}$ and with the projection $\rho^\dagger_q$, mapping each element to its origin. In particular, we shall identify $\mathcal{G}^\dagger(\mathcal{V}, 0)$ with $\mathcal{V}$.

We shall construct a system of coordinates on $\mathcal{G}^\dagger(\mathcal{V}, q)$. Let $\omega^1, \cdots, \omega^q$ be linearly independent elements in Ω. Set

$$(5)^\dagger \quad \mathcal{U}^\dagger(\omega^1, \cdots, \omega^q) \\ = \{E^\dagger \in \mathcal{G}^\dagger(\mathcal{V}, q); \langle \omega^1, E^\dagger \rangle, \cdots, \langle \omega^q, E^\dagger \rangle \text{ are linearly independent}\}.$$

Let $L_r(E^\dagger)$ $(r=1,\cdots,q)$, be the elements in $E^\dagger$ defined by the formula

$$(6)^\dagger \qquad \langle \omega^{r'}, L_r(E^\dagger)\rangle = \delta_r{}^{r'}, \qquad (r, r'=1,\cdots,q)$$

Define the functions ${}^q w_r{}^h$, $(r=1,\cdots q; h=1,\cdots,p-q)$, on $\mathfrak{U}^\dagger(\omega^1,\cdots,\omega^q)$ by the formula

$$(46) \qquad {}^q w_r{}^h(E^\dagger) = \langle w^{q+h}, L_r(E^\dagger)\rangle, \qquad (E^\dagger \in \mathfrak{G}^\dagger(\mathfrak{V},q)).$$

If $(x_1,\cdots,x_n)$ is a system of coordinates on $\mathfrak{V}$, then

$$(x_1 \circ \rho^\dagger{}_q, \cdots, x_n \circ \rho^\dagger{}_q, \cdots, {}^q w_r{}^h, \cdots)$$

is a system of coordinates on $\mathfrak{U}^\dagger(\omega^1,\cdots,\omega^q)$.

In the remainder of the present paper, $(\omega^1,\cdots,\omega^p)$ represents a base of Ω. Then there is an analytic mapping $\eta^\dagger{}_q$ of $\mathfrak{U}^\dagger(\omega^1,\cdots,\omega^q)$ onto $\mathfrak{U}^\dagger(\omega^1,\cdots,\omega^{q-1})$ defined by the formula: for $E^\dagger \in \mathfrak{U}^\dagger(\omega^1,\cdots,\omega^q)$

$$(47) \qquad \eta^\dagger{}_q(E^\dagger) = \text{the space spanned by } L_1(E^\dagger),\cdots,L_{q-1}(E^\dagger).$$

Then clearly

$$(48) \qquad {}^{q-1}w_r{}^{h+1} \circ \eta^\dagger{}_q = {}^q w_r{}^h \qquad (r=1,\cdots,q-1; h=1,\cdots,p-q).$$

Let $\mathfrak{U}^\dagger$ be an open subset in $\mathfrak{G}^\dagger(\mathfrak{V},q)$. By a cross-section of $\mathfrak{G}^\dagger(\mathfrak{V},q)$ into $\mathcal{E}^\dagger\mathfrak{V}$ over $\mathfrak{U}^\dagger$, we mean an analytic mapping X of $\mathfrak{U}^\dagger$ into $\mathcal{E}_x{}^\dagger\mathfrak{V}$ such that $\rho^\dagger \circ X = \rho^\dagger{}_q$. Since $\mathcal{E}^\dagger{}_x\mathfrak{V}$ is a module, it is clear that the set $\mathbf{X}^q(\mathfrak{U}^\dagger,\Omega)$ of all cross-section of $\mathfrak{G}^\dagger(\mathfrak{V},q)$ into $\mathcal{E}^\dagger\mathfrak{V}$ over $\mathfrak{U}^\dagger$ forms a module over the ring $\Lambda^0\mathfrak{U}^\dagger$ of all analytic functions on $\mathfrak{U}^\dagger$. If $\mathfrak{U}^{\dagger\prime} \subset \mathfrak{U}^\dagger$, the restrictions of cross-sections over $\mathfrak{U}^\dagger$ to $\mathfrak{U}^{\dagger\prime}$ induces an additive mapping ${}^\iota\mathfrak{u}^\dagger,\mathfrak{u}^{\dagger\prime}$: $\mathbf{X}^q(\mathfrak{U},\Omega) \to \mathbf{X}^q(\mathfrak{U}^{\dagger\prime},\Omega)$. If $\mathfrak{U}^{\dagger\prime\prime} \subset \mathfrak{U}^\dagger$, then clearly ${}^\iota\mathfrak{u}^{\dagger\prime},\mathfrak{u}^{\dagger\prime\prime} \circ {}^\iota\mathfrak{u}^\dagger,\mathfrak{u}^{\dagger\prime} = {}^\iota\mathfrak{u}^\dagger,\mathfrak{u}^{\dagger\prime\prime}$. By the classical theorem of analytic functions, the mapping ${}^\iota\mathfrak{u}^\dagger,\mathfrak{u}^{\dagger\prime}$ is univalent. Denote by $X^q{}_i(\omega^1,\cdots,\omega^p)$ $(i=1,\cdots,q)$, the element in $X^q(\mathfrak{G}^\dagger(\mathfrak{V},q),\Omega)$ defined by the formula

$$(49) \qquad [X^q{}_i(\omega^1,\cdots,\omega^p)](E^\dagger) = L_i(\mathcal{E}_x{}^\dagger\mathfrak{V}), \quad (x=\rho_q(E^\dagger); E^\dagger \in \mathfrak{G}^\dagger(\mathfrak{V},q))$$

Let $X^q{}_i(\omega^1,\cdots,\omega^p;\mathfrak{U}^\dagger)$ be the restriction of $X^q{}_i(\omega^1,\cdots,\omega^p)$ to $\mathfrak{U}^\dagger$. Then it is easy to see the following:

Proposition III. 1. Let $\mathfrak{U}^\dagger$ be a connected open subset of $\mathfrak{G}^\dagger(\mathfrak{V},q)$. Then the $\Lambda^0\mathfrak{U}^\dagger$-module $\mathbf{X}^q(\mathfrak{U},\Omega)$ is equal to the direct sum of the $\Lambda^0\mathfrak{U}^\dagger \cdot \mathbf{X}^q{}_i$, $(i=1,\cdots,p)$, where $\mathbf{X}^q{}_i = \mathbf{X}^q{}_i\,(\omega^1,\cdots,\omega^p;\mathfrak{U}^\dagger)$.

An element X in $\mathbf{X}^q(\mathfrak{U}^\dagger,\Omega)$ is called proper, if $X(E^\dagger) \in E^\dagger$ for any $E^\dagger \in \mathfrak{U}^\dagger$. Let $\mathfrak{X}^q(\mathfrak{U}^\dagger,\Omega)$ be the set of all proper cross-section over $\mathfrak{U}^\dagger$.

$\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$ is a $\Lambda^0\mathcal{U}^\dagger$-submodule of $X^q(\mathcal{U},\Omega)$. Suppose that $\mathcal{U}^\dagger\subseteq\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$. Then

$$\mathcal{X}^q{}_r(\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)=X^q{}_r(\omega^1,\cdots,\omega^p,\mathcal{U}^\dagger)+\sum_{h=1}^{p-q}{}^q w_r{}^h\cdot X^q{}_{q+h}(\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)$$

is in $\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$, where ${}^q w_r{}^h$ is the function defined by the formula (46).

Proposition III.2. Let $\mathcal{U}^\dagger$ be a connected open set in $\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$. Set $\mathcal{X}^q{}_r=\mathcal{X}^q{}_r(\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)$. Then $\Lambda^0\mathcal{U}^\dagger$-module $\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$ is equal to the direct sum of the $\Lambda^0\mathcal{U}^\dagger\cdot\mathcal{X}^q{}_r$ $(r=1,\cdots,q)$.

For any manifold $\mathcal{V}$, let $[\Lambda^0]\mathcal{V}$ be the field of real meromorphic functions on $\mathcal{V}$. $[\Lambda^0]\mathcal{V}$ is equal to the field of quotient of $\Lambda^0\mathcal{V}$. Set $[X^q](\mathcal{U}^\dagger,\Omega)=[\Lambda^0]\mathcal{U}^\dagger\underset{\Lambda^0\mathcal{U}^\dagger}{\otimes}X^q(\mathcal{U}^\dagger,\Omega)$, the tensor product of $[\Lambda^0]\mathcal{U}^\dagger$ and $X^q(\mathcal{U}^\dagger,\Omega)$ over $\Lambda^0\mathcal{U}^\dagger$. Set $[\mathfrak{X}^q](\mathcal{U}^\dagger,\Omega)=[\Lambda^0]\mathcal{U}^\dagger\underset{\Lambda^0\mathcal{U}^\dagger}{\otimes}\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$. We can naturally identify $X^q(\mathcal{U}^\dagger,\Omega)$ and $\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$ with submodules of $[X^q](\mathcal{U}^\dagger,\Omega)$ and $[\mathfrak{X}^q](\mathcal{U}^\dagger,\Omega)$, respectively. By Propositions III.1 and III.2, we have

Proposition III.3. $[X^q](\mathcal{U}^\dagger,\Omega)$ is a vector space over the field $[\Lambda^0]\mathcal{U}^\dagger$ of p dimensions. Then the $X_i(\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)$ $(i=1,\cdots,p)$, form a base of $[X^q](\mathcal{U}^\dagger,\Omega)$. If, moreover, $\mathcal{U}^\dagger$ is contained in $\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$, then $[\mathfrak{X}^q](\mathcal{U}^\dagger,\Omega)$ is a vector space over $[\Lambda^0]\mathcal{U}^\dagger$ of dimension q and the $\mathcal{X}_r{}^q(\omega^1,\cdots,\omega^1;\mathcal{U}^\dagger)$ $(r=1,\cdots,q)$, form a base of it.

2. Ideals associated with a normal system. Let (Σ,Ω) be a normal system over $\mathcal{V}$. Let p be the number of independent variables in Ω. For any subset Λ of $\Lambda^1\mathcal{V}$ and for any open subset $\mathcal{U}^\dagger$ of $\mathcal{G}^\dagger(\mathcal{V},q)$, denote by $(\Lambda,\mathcal{U}^\dagger)$ the $\Lambda^0\mathcal{U}^\dagger$-submodule of $\Lambda^1\mathcal{U}^\dagger$ generated by all $\rho_q{}^{\dagger *}\theta$, $(\theta\in\Lambda)$. Set

$$Y^q(\Sigma,\mathcal{U}^\dagger)=(\Lambda^1\mathcal{V},\mathcal{U}^\dagger)/(\Sigma^{[1]}+\Omega,\mathcal{U}^\dagger) \tag{50}$$

$Y^q(\Sigma,\mathcal{U}^\dagger)$ is a module over the ring $\Lambda^0\mathcal{U}^\dagger$. If $\mathcal{U}^{\dagger\prime}\subseteq\mathcal{U}^\dagger$, there is an univalent additive mapping ${}^\iota\mathcal{U}^\dagger,\mathcal{U}^{\dagger\prime}$: $Y^q(\Sigma,\mathcal{U}^\dagger)\to Y^q(\Sigma,\mathcal{U}^{\dagger\prime})$. Set

$$[Y^q](\Sigma,\mathcal{U}^\dagger)=[\Lambda^0]\mathcal{U}^\dagger\underset{\Lambda^0\mathcal{U}^\dagger}{\otimes}Y^q(\Sigma,\mathcal{U}^\dagger).$$

$[Y^q](\Sigma,\mathcal{U}^\dagger)$ is a vector space over $[\Lambda^0]\mathcal{U}^\dagger$. By the condition (ii) of normal systems, one sees easily that $Y^q(\Sigma,\mathcal{U}^\dagger)$ is torsion free. Therefore we can naturally identity $Y^q(\Sigma,\mathcal{U}^\dagger)$ with a submodule of $[Y^q](\Sigma,\mathcal{U}^\dagger)$. For any ϖ in $\Lambda^1\mathcal{V}$, set

(51) $\{\varpi\}_q=$ (the class modulo $(\Sigma^{[1]}+\Omega,\mathcal{U}^\dagger)$ containing $(\rho_q{}^\dagger)^*\varpi$).

We remark that, by Definition II. 1, there is a base of $\Lambda^1\mathfrak{V}$-modulo $\Sigma^{[1]}+\Omega$. This base consists of m elements.

Proposition III. 4. $[Y^q](\Sigma,\mathfrak{U}^\dagger)$ is a vector space of dimension m over $[\Lambda^0]\mathfrak{U}^\dagger$.

Let $\varpi^1,\cdots,\varpi^m$ be a base of $\Lambda^1\mathfrak{V}$ modulo $\Sigma^{[1]}+\Omega$. Then $\{\varpi^1\}_q,\cdots,\{\varpi^m\}_q$ form a base of $[Y^q](\Sigma,\mathfrak{U}^\dagger)$. $Y^q(\Sigma,\mathfrak{U}^\dagger)$ is equal to the direct sum of $\Lambda^0\mathfrak{U}^\dagger\cdot\{\varpi^\lambda\}_q$ $(\lambda=1,\cdots,m)$.

Denote by $[Z](\Sigma,\mathfrak{U}^\dagger)$ the (abstract) direct sum of the vector space $[Y^q](\Sigma,\mathfrak{U}^\dagger)+[X^q](\mathfrak{U}^\dagger,\Omega)$. Let

$$\mathfrak{P}_q(\Sigma,\mathfrak{U}^\dagger) \tag{52}$$

be the symmetric algebra over $[Z](\Sigma,\mathfrak{U}^\dagger)$. Thus if we choose bases $\omega^1,\cdots,\omega^p$ and $\varpi^1,\cdots,\varpi^m$ of Ω and of Λ^1V modulo $\Sigma^{[1]}+\Omega$, and if we set $X_i=X_i^q(\omega^1,\cdots,\omega^p;\mathfrak{U}^\dagger)$ and $Y^\lambda=\{\varpi^\lambda\}_q$, then the elements in $\mathfrak{P}_q(\Sigma,\mathfrak{U}^\dagger)$ are expressed as polynomials $X_1,\cdots,X_p$, $Y^1,\cdots,Y^m$ with coefficients in $[\Lambda^0]\mathfrak{U}^\dagger$. Let

$$\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger) \tag{53}$$

by the subring of $\mathfrak{P}_q(\Sigma,\mathfrak{U}^\dagger)$ which is $\Lambda^0\mathfrak{U}^\dagger$-generated by $Y^q(\Sigma,\mathfrak{U}^\dagger)$ and $X^q(\mathfrak{U}^\dagger,\Omega)$. Thus the elements in $\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger)$ are expressed as polynomials in $X_1,\cdots,X_p$, $Y^1,\cdots,Y^m$ with coefficients in $\Lambda^0\mathfrak{U}^\dagger$.

By Definition II. 1, we can write any $\phi\in\Sigma^{[2]}$ as

$$\phi\equiv\sum_{i=1}^{p}\sum_{\lambda=1}^{m}A_{\phi\,;i\lambda}\omega^i\wedge\varpi^\lambda+\sum_{i=1}^{p}\sum_{j=1}^{p}\tfrac{1}{2}B_{\phi\,;ij}\omega^i\wedge\omega^j \quad (\mathrm{mod}\,\Sigma^{[1]}), \tag{24}$$

where $A_{\phi\,;i\lambda}$ and $B_{\phi\,;ij}$ are in $\Lambda^0\mathfrak{V}$ and $B_{\phi\,;ij}+B_{\phi\,;ji}=0$. Then

$$P_{\phi\,;ij}=\sum_{\lambda=1}^{m}(A_{\phi\,;i\lambda}\circ\rho_q{}^\dagger)\cdot Y^\lambda\cdot X_j-(A_{\phi\,;j\lambda}\circ\rho_q{}^\dagger)\cdot Y^\lambda\cdot X_i$$

is an element in $\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger)$. Of course, $P_{\phi\,;ij}$ depends on the choice of the bases $\omega^1,\cdots,\omega^p$ and $\varpi^1,\cdots,N^m$. But one can verify easily that the $\Lambda^0\mathfrak{U}^\dagger$-submodule $S_q(\mathfrak{U}^\dagger)$ of $P'_q(\Sigma,\mathfrak{U}^\dagger)$ generated by all $P_{\phi\,;ij}$, $(\phi\in\Sigma^{[2]})$, does not depend on the choice of the bases. Denote by $T_q(\mathfrak{U}^\dagger)$ the $\Lambda^0\mathfrak{U}^\dagger$-submodule of $\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger)$ generated by all $Y\cdot X$, where Y and X run through $Y^q(\Sigma,\mathfrak{U}^\dagger)$ and $X^q(\mathfrak{U}^\dagger,\Omega)$, respectively. When $q=0$, $T_q(\mathfrak{U}^\dagger)$ is defined to be 0.

Definition III. 1. $A_q(\Sigma,\mathfrak{U}^\dagger)$ is defined to be the ideal in $\mathfrak{P}_q(\Sigma,\mathfrak{U}^\dagger)$ generated by $S_q(\mathfrak{U}^\dagger)$ and $T_q(\mathfrak{U}^\dagger)$, $(q=0,1,\cdots,p-1)$. $A'_q(\Sigma,\mathfrak{U}^\dagger)$ is defined to be the ideal in $\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger)$ generated by $S_q(\mathfrak{U}^\dagger)$ and $T_q(\mathfrak{U}^\dagger)$.

Definition III. 2. $B_q(\Sigma, \mathcal{U}^\dagger)$ is defined to be the product of $\mathbf{Y}^q(\Sigma, \mathcal{U}^\dagger)$ and $A^q(\Sigma, \mathcal{U}^\dagger)$. $B'_q(\Sigma, \mathcal{U}^\dagger)$ is defined to be the product of $Y^q(\Sigma, \mathcal{U}^\dagger)$ and $A'_q(\Sigma, \mathcal{U}^\dagger)$.

Proposition III. 5. Let $\mathcal{U}^\dagger$ be an open connected subset of $\mathcal{U}^\dagger(\omega^1, \cdots, \omega^q)$, (cf. (5)†). Set $X_i = X_i{}^q(\omega^1, \cdots, \omega^p; \mathcal{U}^\dagger)$. Let $\varpi^1, \cdots, \varpi^m$ be a base of $\Lambda^1\mathcal{V}$ modulo $\Sigma^{[1]} + \Omega$. Set $Y^\lambda = \{\varpi^\lambda\}_q$, (cf. (51)). Define the function ${}^q w_r{}^h$ on $\mathcal{U}^\dagger$ by the formula (46). Then $A_q(\Sigma, \mathcal{U}^\dagger)$ and $A'_q(\Sigma, \mathcal{U}^\dagger)$ are generated by all

$$\begin{aligned}
&\xi_{\phi;ij}(\mathcal{U}^\dagger) = \sum_{\lambda=1}^{m} (A_{\phi;i\lambda} X_j - A_{\phi;j\lambda} X_i) Y^\lambda,\\
(54)\qquad &\zeta_r{}^\lambda(\mathcal{U}^\dagger) = (X_r + \sum_{h=1}^{p-q} {}^q w_r{}^h \cdot X_{q+h}) Y^\lambda,
\end{aligned}$$

($\lambda = 1, \cdots, m$; $i, j = 1, \cdots, p$; $r = 1, \cdots, q$) (cf. Proposition III. 2 and 3).

Let x be a point of $\mathcal{V}$. Set $Y(x) = \langle \Lambda^1\mathcal{V}, \mathcal{E}_x\mathcal{V}\rangle / \langle \Sigma^{[1]} + \Omega, \mathcal{E}_x\mathcal{V}\rangle$. Let

$$(55)\qquad P(x)$$

be the symmetric algebra over the direct sum $Y(x) + \mathcal{E}^\dagger{}_x\mathcal{V}$. If we take bases $X_1, \cdots, X_p$, and $Y^1, \cdots, Y^m$ of $\mathcal{E}^\dagger{}_x\mathcal{V}$ and $Y(x)$, then $P(x)$ is canonically isomorphic to the polynomial ring $\boldsymbol{R}[X_1, \cdots, X_p, Y^1, \cdots, Y^m]$. Let $E^\dagger$ be a q dimensional reduced contact element to $\mathcal{V}$ at x. Then taking the value at $E^\dagger$, we can define, for any $E^\dagger \in \mathcal{U}^\dagger$, a homomorphism

$$\kappa_{E^\dagger}\colon \mathcal{P}'_q(\Sigma, \mathcal{U}^\dagger) \to P(x).$$

More explicitly, if one take bases $\omega^1, \cdots, \omega^p$ and $\varpi^1, \cdots, \varpi^m$ of Ω and of $\Lambda^1 V$ modulo $\Sigma^{[1]} + \Omega$, respectively, then $\kappa_{E^\dagger}$ is defined by the following formulas:

$$\begin{aligned}
&\kappa_{E^\dagger}(f) = f(E^\dagger), \qquad (f \in \Lambda^0\mathcal{U}^\dagger),\\
(56)\qquad &\kappa_{E^\dagger}(\{\varpi^\lambda\}_q) = (\langle \varpi^\lambda, \mathcal{E}_x\mathcal{V}\rangle \bmod \langle \Sigma^{[1]} + \Omega, \mathcal{E}_x\mathcal{V}\rangle),\\
&\kappa_{E^\dagger}(X_i{}^q(\omega^1, \cdots, \omega^p; \mathcal{U}^\dagger)) = L_i(\mathcal{E}^\dagger{}_x\mathcal{V}).
\end{aligned}$$

Clearly, if $\mathcal{U}^\dagger \supseteq \mathcal{U}^{\dagger\prime}$, then $\kappa_{E^\dagger}(A'_q(\Sigma, \mathcal{U}^{\dagger\prime})) \supseteq \kappa_{E^\dagger}(A'_q, \mathcal{U}^\dagger))$. Set

$$(57)\qquad A(E^\dagger) = \bigcup \{\kappa_{E^\dagger}(A'_q(\Sigma, \mathcal{U}^\dagger)); \mathcal{U}^\dagger \text{ connected open neighborhood of } E^\dagger \text{ in } \mathcal{G}^\dagger(\mathcal{V}, q)\}.$$

$A(E^\dagger)$ is an ideal in $P(x)$. Set $X_i = [X^q{}_i(\omega^1, \cdots, \omega^p)](E^\dagger)$, (ct. (50)). Set $Y^\lambda = \langle \varpi^\lambda, \mathcal{E}_x\mathcal{V}\rangle$ modulo $\langle \Sigma^{[1]} + \Omega, \mathcal{E}_x\mathcal{V}\rangle$. These are elements in $P(x)$. Set

$$(58)\qquad \xi_{\phi;ij}(E^\dagger) = \sum_{h=1}^{p-q} (A_{\phi;i\lambda}(x) \cdot Y^\lambda \cdot X_j - \mathrm{A}_{\phi;i\lambda}(x) \cdot Y^\lambda \cdot X_i)$$

Then we have

Proposition III. 6. $A(E^\dagger)$ is generated by all $\xi_{\phi;ij}(E^\dagger)$, $(\phi \in \Sigma^{[2]})$, and by all $Y^\lambda \cdot X$, $(X \in E^\dagger \subset \mathcal{E}^\dagger{}_x \mathfrak{V})$. Assume further that $E^\dagger$ is in

$$\mathfrak{U}^\dagger = \mathfrak{U}^\dagger(\omega^1, \cdots, \omega^q),$$

(cf. $(5)^\dagger$). Then $A(E^\dagger) = \kappa_{E^\dagger}(A'_q(\Sigma, \mathfrak{U}^\dagger))$ and $A(E^\dagger)$ is generated by all $\xi_{\phi;ij}(E^\dagger)$ $(\phi \in \Sigma^{[2]})$, and by all

$$(58)' \qquad \zeta_r{}^\lambda(E^\dagger) = Y^\lambda X_r + \sum_{h=1}^{p-q} {}^q w_r{}^h(E^\dagger) X_{q+h},$$
$$(\lambda = 1, \cdots, m; r = 1, \cdots, q).$$

Similarly, we shall set

$$(59) \qquad B(E^\dagger) = \bigcup \{\kappa_{E^\dagger}(B'_q(\Sigma, \mathfrak{U}^\dagger)), \mathfrak{U}^\dagger \text{ connected open neighborhood of } E^\dagger \text{ in } \mathfrak{G}^\dagger(\mathfrak{V}, q)\}.$$

Then, by the definition of $B'_q(\Sigma, \mathfrak{U}^\dagger)$,

$$(59)' \qquad B(E^\dagger) = Y(x) \cdot A(E^\dagger).$$

3. Hilbert's characteristic functions. Let $X_1, \cdots, X_p$ be p indeterminates. Order monomials $X_1{}^{k_1} \cdots X_p{}^{k_p}$ lexicographically. Let M be the set of all monomials of total degree l smaller than a fixed monomial of total degree l. Let k be the number of elements in M. Denote by $Q_l(k, p)$ the number of elements in the set $MX_1 \cup \cdots \cup MX_p$. It is easy to see that if l is sufficiently large compared with k, $Q_l(k, p)$ depends only on k and p. Thus we can define the integer $Q(k, p) = Q_l(k, p)$ for sufficiently large l. The function $Q(k, p)$ may be called the Macauly's function.

Let K be an arbitrary field and let I be an homogeneous ideal in the polynomial ring $K[X_1, \cdots, X_p]$, "homogeneous" means that $I = \sum_{l=0}^{\infty} I^{[l]}$, $I^{[l]} = I \cap K^{[l]}[X_1, \cdots, X_p]$, where $K^{[l]}[X_1, \cdots, X_p]$ is the submodule of all homogeneous polynomials of degree l. Set $\phi^l(I)$ = the dimension of the vector space $I^{[l]}$.

THEOREM III. 1. (Hilbert-Macauly). *For any homogeneous ideal I in $K[X_1, \cdots, X_p]$, there is an integer $l_0(I)$ satisfying the following conditions:*

$$\text{(i)} \qquad \phi^{l+1}(I) > Q(\phi^l(I), p), \text{ for } l < l_0(I),$$

$$\text{(ii)} \qquad \phi^{l+1}(I) = Q(\phi^l(I), p), \text{ for } l \geqq l_0(I).$$

For the proof, consult S. Bochner [1, p. 8].

When the ring $K[X_1, \cdots, X_p]$ has a double degree, i. e., $K[X_1, \cdots, X_p]$

$=\sum_{a,l} K^{[a,l]}[X_1,\cdots,X_p]$, and if an ideal I is homogeneous with respect to the double degree, we shall set $\phi^{a,l}(I)=$ the dimension of the vector space $I^{[a,l]}$.

The ring $\mathcal{P}_q(\Sigma,\mathcal{U}^\dagger)$ introduced in §2 is a polynomial ring over the field $[\Lambda^0]\mathcal{U}^\dagger$. Let $\mathcal{P}_q^{[l]}(\Sigma,\mathcal{U}^\dagger)$ be the module of all homogeneous polynomials of degree l. It has also a double degree, that is, the degree with respect to $[\mathbf{Y}^q](\Sigma,\mathcal{U}^\dagger)$ and to $[\mathbf{X}^q](\Sigma,\mathcal{U}^\dagger)$. Denote by $\mathcal{P}_q^{[a,l]}(\Sigma,\mathcal{U}^\dagger)$ the submodule of all homogeenous polynomials of degrees a and l with respect to $[\mathbf{Y}^q](\Sigma,\mathcal{U}^\dagger)$ and to $[\mathbf{X}^q](\Sigma,\mathcal{U}^\dagger)$, respectively. Similarly we define $P^{[l]}(x)$, $P^{[a,l]}(x)$. $P^{[a,l]}(x)$ is the submodule of all polynomials of degrees a and l with respect to $Y(x)$ and $\mathcal{E}^\dagger_x\mathcal{V}$, respectively.

Definition III. 3.

$$\phi^l_q(\Sigma,\Omega)=\mathrm{Max}\{\phi^l(A_q(\Sigma,\mathcal{U}^\dagger))\,;\ \mathcal{U}^\dagger \text{ connected open set in } \mathcal{G}^\dagger(\mathcal{V},q)\},$$
$$\psi^l_q(\Sigma,\Omega)=\mathrm{Max}\{\phi^l(B_q(\Sigma,\mathcal{U}^\dagger))\,;\ \mathcal{U}^\dagger \text{ connected open set in } \mathcal{G}^\dagger(\mathcal{V},q)\},$$
$$t^l_q(\Sigma,\Omega)=\phi^{l+1}_q(\Sigma,\Omega)-\psi^{l+1}_q(\Sigma,\Omega).$$
$$\phi^l(\Sigma,E^\dagger)=\phi^l(A(E^\dagger)),\qquad \psi(\Sigma,E^\dagger)=\phi^l(B(E^\dagger)),$$
$$t^l(\Sigma,E^\dagger)=\phi^{l+1}(\Sigma,E^\dagger)-\psi^{l+1}(\Sigma,E^\dagger).$$

Since the dimension of the vector space $\mathcal{P}_q^{[l]}(\Sigma,\mathcal{U}^\dagger)$ is independent of $\mathcal{U}^\dagger$, $\phi^l(\Sigma,\Omega)$ and $\psi^l(\Sigma,\Omega)$ are well defined integers. One sees easily by (59)′ that

$$(60)\qquad t^l(\Sigma,E^\dagger)=\phi^{[1,l]}(A(E^\dagger))$$

Let $\omega^1,\cdots,\omega^p$ be a base of Ω. Let E be an element in $\mathcal{V}_l^q$ (cf. (36)). Let x be the origin of E. Then the set of all $(d\rho^l L \bmod \mathcal{E}^*_x\mathcal{V})$, $L\in E$, forms a q-dimensional reduced contact element $E^\dagger=\mu(E)$ contained in $\mathcal{U}^\dagger=\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$, where ρ^l is the projection of $\mathcal{V}_l^q$ onto $\mathcal{V}$. The mapping

$$(61)\qquad \mu:\ \mathcal{V}_l^q\rightarrow\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$$

is analytic and onto. By (39) and (46), it follows that

$$(60)'\qquad w_r^{q,h}(E)={}^qw_r^h(\mu(E)),\qquad (E\in\mathcal{V}_l^q).$$

Now we claim the following equality

$$(62)\qquad t^r(E)=t^l(\Sigma,\mu(E)),\qquad (E\in\mathcal{V}_l^q).$$

(cf. (45)). To prove (62), denote by S the subspace of the conjugate space of $\mathcal{E}_x\mathcal{R}_l$ generated by all $\langle du^\lambda_{i_1\cdots i_l},\mathcal{E}_x\mathcal{R}\rangle=X^\lambda_{i_1\cdots i_l}$. Then $X^\lambda_{i_1\cdots i_l}=X^\lambda_{j_1\cdots j_l}$ for any permutation $j_1,\cdots,j_l$ of $i_1,\cdots,i_l$, and as far as the

linear relations among $X^{\lambda}{}_{i_1\cdots i_l}$ are concerned, we can think of $X^{\lambda}{}_{i_1\cdots i_l}$ as indeterminates under the conditions of symmetry stated above. Let M be the subspace of S generated by

$$\bar{\xi}^{\lambda}{}_{\phi;ij;k_1\cdots k_{l-1}} = \sum_{\lambda=1}^{m} (A_{\phi;i\lambda}(y) X^{\lambda}{}_{jk_1\cdots k_{l-1}} - A_{\phi;j\lambda}(y) X^{\lambda}{}_{ik_1\cdots k_{l-1}})$$

$$\bar{\zeta}^{\lambda}{}_{k_1\cdots k_{l-1};r} = X^{\lambda}{}_{k_1\cdots k_{l-1}r} + \sum_{h=1}^{p-q} w_r{}^{q,h}(E) X^{\lambda}{}_{k_1\cdots k_{l-1}q+h}$$

$(\phi \in \Sigma^{[2]};\ \lambda = 1,\cdots, m;\ i, j, k_1,\cdots, k_{l-1} = 1,\cdots, p;\ r = 1,\cdots, q)$, where $y = \rho^l(x)$. Then by (45)

$$(62)' \qquad t'(E) = \dim M.$$

Set $E^{\dagger} = \mu(E)$. Then

$$(62)'' \qquad t(\Sigma, E^{\dagger}) = \dim (A(E^{\dagger})^{[1,l]}).$$

By Proposition III.6, $A(E^{\dagger})^{[1,l]}$ is a subspace of the vector space $(P(x))^{[1,l]}$ generated by all

$$\xi_{\phi;ij}(E^{\dagger}) \cdot X_{k_1} \cdots X_{k_{l-1}} = \sum_{\lambda=1}^{m} (A_{\phi;i\lambda}(y) Y^{\lambda} X_j X_{k_1} \cdots X_{k_{l-1}} - A_{\phi;j\lambda}(y) Y^{\lambda} X_i X_{k_1} \cdots X_{k_{l-1}})$$

$$\zeta^{\lambda}{}_r(E^{\dagger}) \cdot X_{k_1} \cdots X_{k_{l-1}} = Y^{\lambda} X_{k_1} \cdots X_{k_{l-1}} X_r + \sum_{h=1}^{p-q} {}^q w_r{}^h (E^{\dagger}) Y^{\lambda} X_{k_1} \cdots X_{k_{l-1}} X_{q+h}$$

$(\phi \in \Sigma^{[2]};\ \lambda = 1,\cdots, m;\ i, j, k_1,\cdots, k_{l-1} = 1,\cdots, p;\ r = 1,\cdots, q)$. Let a be the homomorphism of S onto the vector space $(P(x))^{[1,l]}$ defined by formulas: $a(Y^{\lambda} X_{k_1} \cdots, X_{k_l}) = X^{\lambda}{}_{k_1\cdots k_l}$. Then, by the remark in the beginning of this proof, a is an isomorphism. Comparing the system of generators of M and $(A(E^{\dagger})^{[1,l]})$, we see by (60)′ that a maps $A(E^{\dagger})$ upon M. Hence, by (62)′ and (62)″, the equality (62) holds.

LEMMA III.1. *Let $\mathfrak{W}$ be a real analytic manifold. Take a system of indeterminates $W_1,\cdots, W_a$. Let $F_1,\cdots, F_p$ be linear elements in $(\Lambda^0\mathfrak{W})[W_1,\cdots, W_a]$, that is, linear combinations of $W_1,\cdots, W_a$ with coefficient analytic functions on $\mathfrak{W}$. Let $\mathfrak{D}$ be a connected open subset of $\mathfrak{W}$. Then F_i is considered as an element in $(\Lambda^0\mathfrak{D})[W_1,\cdots, W_a]$, by restriction. If there is $\mathfrak{D}$ such that $F_1,\cdots, F_b$ have a non-trivial linear relation in $(\Lambda^0\mathfrak{D})[W_1,\cdots, W_a]$, then $F_1,\cdots, F_b$ have also a non-trivial linear relation in $(\Lambda^0\mathfrak{W})[W_1,\cdots, W_a]$.*

Proof. By the restriction mapping, we can identify $K_1 = [\Lambda^0]\mathfrak{W}$ with a subfield of $K = [\Lambda^0]\mathfrak{D}$. This follows from the theorem of identity in the

theory of functions of several complex variables. Set $F_i = \alpha^{\mu}{}_i W_{\mu}$, $\alpha^{\mu}{}_i \in K_1$. Assume that $\beta^i F_i = 0$, $\beta^i \in K$. Since K can be considered as a vector space over the field K_1, there is a base $\{e^{\sigma}\}$ such that any $\beta \in K$ can be expressed uniquely as $\beta = \beta_{\sigma} e^{\sigma}$, where $\beta_{\sigma} \in K_1$ and, for almost all σ, β_{σ} is zero. Set $\beta^i = \beta_{\sigma}{}^i e^{\sigma}$. Then $\beta^i F_i = 0$ implies that $\beta_{\sigma}{}^i F_i = 0$ for all σ. Then it follows easily that $F_1, \cdots, F_n$ have a non-trivial linear relation in $(\Lambda^0 \mathcal{W})[W_1, \cdots, W_n]$.

Proposition III. 7. Let $\omega^1, \cdots, \omega^q$ be linearly independent elements in Ω. Then, for any open connected set $\mathcal{U}^{\dagger}$ contained in $\mathcal{U}^{\dagger}(\omega^1, \cdots, \omega^q)$, $\phi^l(A_q(\Sigma, \mathcal{U}^{\dagger})) = \phi^l(\Sigma, \Omega)$ and $\psi^l(B_q(\Sigma\, \mathcal{U}^{\dagger})) = \psi^l(\Sigma, \Omega)$ and $t_q{}^l(\Sigma, \Omega = \phi^{[1,l]}(A_q(\Sigma, \mathcal{U}^{\dagger}))$.

Proof. We shall show first that, for any connected open sets $\mathcal{U}^{\dagger\prime} \subset \mathcal{U}^{\dagger}$, $\phi^l(A_q(\Sigma, \mathcal{U}^{\dagger})) = \phi^l(A_q(\Sigma, \mathcal{U}^{\dagger\prime}))$. By Proposition III. 5, there is a system of generators $F_1, \cdots, F_b$ of $A_q(\Sigma, \mathcal{U}^{\dagger})$ such that the restrictions of $F_1, \cdots, F_b$ to $\mathcal{U}^{\dagger\prime}$ form a system of generators of $A_q(\Sigma, \mathcal{U}^{\dagger\prime})$. Then our contention follows from Lemma III. 1. In particular, we have

$$\phi^l(A_q(\Sigma, \mathcal{U}^{\dagger})) = \phi^l(A_q(\Sigma, \mathcal{U}^{\dagger}(\omega^1, \cdots, \omega^q))).$$

Lemma III. 1 implies that, for any connected open subsets $\mathcal{W}^{\dagger\prime} \subseteq \mathcal{W}^{\dagger}$, $\phi^l(A_q(\Sigma, \mathcal{W}^{\dagger\prime})) \geqq \phi^l(A_q(\Sigma, \mathcal{W}^{\dagger}))$. Assume that $\phi^l{}_q(\Sigma, \Omega) = \phi^l(A_q(\Sigma, \mathcal{W}^{\dagger}))$. Since $\mathcal{U}^{\dagger}(\omega^1, \cdots, \omega^q)$ is everywhere dense in $\mathcal{G}^{\dagger}(\mathcal{V}, q)$, there is a connected open set $\mathcal{U}^{\dagger}$ in $\mathcal{U}^{\dagger}(\omega^1, \cdots, \omega^q) \cap \mathcal{W}^{\dagger}$. Then $\phi^l(A_q(\Sigma, \mathcal{U}^{\dagger})) = \phi^l{}_q(\Sigma, \Omega)$. Therefore for any $\mathcal{U}^{\dagger\prime}$ in $\mathcal{U}^{\dagger}(\omega^1, \cdots, \omega^q)$, $\phi^l{}_q(\Sigma, \Omega) = \phi^l(A_q(\Sigma, \mathcal{U}^{\dagger\prime}))$. The same argument proves the second equality. The third equality follows from the first two equalities and Definition III. 2.

By Proposition III. 7, the integer $l_0(A_q(\Sigma, \mathcal{U}^{\dagger}(\omega^1, \cdots, \omega^q)))$ (defined in Theorem III. 1) does not depend on the choice of $\omega^1, \cdots, \omega^q$. This integer will be denoted by $l_0(\Sigma, \Omega)$,

$$l_0(\Sigma, \Omega) = l_0(A_q(\Sigma, \mathcal{U}^{\dagger}(\omega^1, \cdots, \omega^q))). \tag{63}$$

LEMMA III. 2. *Let $\omega^1, \cdots, \omega^p$ be a base of Ω. Set $\mathcal{U}^{\dagger} = \mathcal{U}^{\dagger}(\omega^1, \cdots, \omega^q)$. Let $F_1, \cdots, F_b$ be elements in $\mathcal{P}'_q(\Sigma, \mathcal{U}^{\dagger})$. Take $E^{\dagger}$ in $\mathcal{G}^{\dagger}$. If $\kappa_{E^{\dagger}}(F_1), \cdots, \kappa_{E^{\dagger}}(F_b)$ are linear independent, then $F_1, \cdots, F_b$ are also linearly independent in $\mathcal{P}_q(\Sigma, \mathcal{U}^{\dagger})$.*

Proof. There is a neighborhood $\mathcal{N}^{\dagger}$ of $E^{\dagger}$ such that, for any $E^{\dagger\prime} \in \mathcal{N}^{\dagger}$, $\kappa_{E^{\dagger\prime}}(F_1), \cdots, \kappa_{E^{\dagger\prime}}(F_b)$ are also linearly independent. If $F_1, \cdots, F_b$ are not linearly independent, there is a non-trivial relation $\beta_1 F_1 + \cdots + \beta_b F_b = 0$, β_i is an analytic function on $\mathcal{U}^{\dagger}$. There is $E^{\dagger\prime}$ in $\mathcal{N}^{\dagger}$ such that $\beta_i(E^{\dagger\prime}) \neq 0$

for $i=1,\cdots,b$. Then $\kappa_{E^{\dagger\prime}}(F_1),\cdots,\kappa_{E^{\dagger\prime}}(F_b)$ are not linearly independent, which contradicts to the choice of $\mathfrak{N}^{\dagger}$.

Proposition III. 8. Let $E^{\dagger}$ be an element in $\mathfrak{G}^{\dagger}(\mathfrak{V}^{\dagger},q)$. Then,

(i) $$\phi^l(\Sigma,E^{\dagger})\leqq\phi^l{}_q(\Sigma,\Omega):$$

(ii) if $\phi^l(\Sigma,E^{\dagger})=\phi^l{}_q(\Sigma,\Omega)$, then $\psi^l(\Sigma,E^{\dagger})=\psi^l{}_q(\Sigma,\Omega)$;

(iii) if $E^{\dagger}\in\mathfrak{U}^{\dagger}=\mathfrak{V}^{\dagger}(\omega^1,\cdots,\omega^q)$ and if $F_1,\cdots,F_b$ are elements of degree l in $A'_q(\Sigma,\mathfrak{U}^{\dagger})$ such that $\kappa_{E^{\dagger}}(F_1),\cdots,\kappa_{E^{\dagger}}(F_b)$ form a base of $A^{[l]}(E^{\dagger})$, then $\phi^l(\Sigma,E^{\dagger})=\phi^l{}_q(\Sigma,\Omega)$ when and only when $F_1,\cdots,F_b$ a base of $A_q{}^{[l]}(\Sigma,\mathfrak{U}^{\dagger})$.

Proof. (i) and (iii) follow from Lemma III. 2. (ii) follows from Proposition III. 7.

4. P-regular points. Let (Σ,Ω) be a normal system on $\mathfrak{V}$. Let p be the number of independent variables. A point x of $\mathfrak{V}$ is called a $\mathfrak{P}$-semi-regular point of order l with respect to (Σ,Ω) if, for any $q=0,1,\cdots,p-1$, there is a q dimensional reduced contact element $E_q{}^{\dagger}$ to $\mathfrak{V}$ at x such that $\phi^{l+1}(\Sigma,E_q{}^{\dagger})=\phi^{l+1}{}_q(\Sigma,\Omega)$. A point x is called a $\mathfrak{P}$-regular point (with respect to (Σ,Ω)) if there is an integer l_0 such that x is a $\mathfrak{P}$-semi-regular point of order l for every $l\geqq l_0$. l_0 will be called a weight of the $\mathfrak{P}$ regular point x.

Set

(64) $$S(\Sigma,\Omega,l)=\{\text{the set of all points which are not } \mathfrak{P}\text{-semi-regular points of order } l\};$$

(65) $$S(\Sigma,\Omega)=\{\text{the set of all points which are not } \mathfrak{P}\text{-regular points}\}.$$

Clearly we have

(66) $$S(\Sigma,\Omega)=\bigcap_{l_0}\Big[\bigcup_{l\geqq l_0}S(\Sigma,\Omega,l)\Big].$$

Definition III. 5. Let x be a point in $\mathfrak{V}$. Let $F^{\dagger}$ be a flag on $\mathfrak{E}^{\dagger}{}_x\mathfrak{V}$ (Definition I. 11). Denote by $E_q{}^{\dagger}$ the q-th component of $F^{\dagger}$ $(q=0,1,\cdots,p-1)$. $F^{\dagger}$ is called a regular reduced flag (with respect to (Σ,Ω)), if there is an integer l_0 such that $\phi^{l+1}{}_q(\Sigma,\Omega)=\phi^{l+1}(\Sigma,E_q{}^{\dagger})$ for any $l\geqq l_0$ and any $q=0,1,\cdots,p-1$. l_0 will be called the weight of the regular reduced flag $F^{\dagger}$.

Denote by $\mathfrak{F}^{\dagger}(x)$ the set of all flags on $\mathfrak{E}^{\dagger}{}_x\mathfrak{V}$. Set $\mathfrak{F}^{\dagger}\mathfrak{V}=\bigcup\{\mathfrak{F}(x);x\in\mathfrak{V}\}$. $\mathfrak{F}^{\dagger}\mathfrak{V}$ is an analytic manifold and $\mathfrak{F}^{\dagger}(x)$ is a submanifold of $\mathfrak{F}^{\dagger}\mathfrak{V}$. The main theorems of this section are the following:

THEOREM III. 2. *$S(\Sigma,\Omega)$ and $S(\Sigma,\Omega,l)$ are proper subvarieties of $\mathfrak{V}$.*

THEOREM III. 3. *Let x be a $\mathfrak{P}$-semi-regular point of order l' with respect to (Σ,Ω). If $l' \geqq l_0(\Sigma,\Omega)$, then x is a $\mathfrak{P}$-regular point of weight l'* (cf. (63)).

THEOREM III. 4. *Let x be a $\mathfrak{P}$-regular point of weight l_0. Assume that $l_0 \geqq l_0(\Sigma,\Omega)$. Then there is a regular reduced flag $F^\dagger$ on $\mathcal{E}^\dagger{}_x\mathfrak{V}$ of weight l_0. Moreover, the set $\mathcal{R}\mathcal{F}^\dagger(\mathfrak{V};l_0)$ of all reduced regular flags of weight l_0 is an open set in $\mathcal{F}^\dagger\mathfrak{V}$.*

LEMMA III. 3. *Denote by $S(\Sigma,\Omega,l;q)$ the set of all $E^\dagger$ in $\mathfrak{G}^\dagger(\mathfrak{V},q)$ such that $\phi^{l+1}(\Sigma,E^\dagger) < \phi^{l+1}(\Sigma,\Omega)$. Then $S(\Sigma,\Omega,l;q)$ is a proper subvariety of $\mathfrak{G}^\dagger(\mathfrak{V},q)$.*

Proof. Take a base $\omega^1,\cdots,\omega^p$ of Ω. Set $\mathfrak{U}^\dagger = \mathfrak{U}(\omega^1,\cdots,\omega^p)$. It is sufficient to show that $S(\Sigma,\Omega,l;q) \cap \mathfrak{U}^\dagger$ is a proper subvariety of $\mathfrak{U}^\dagger$, since $\mathfrak{U}^\dagger$ is an open subset of $\mathfrak{G}^\dagger(\mathfrak{V},q)$ and $\mathfrak{G}^\dagger(\mathfrak{V},q)$ is covered by such $\mathfrak{U}^\dagger$'s. It is clear by Proposition III. 5 and (56) that, for any linearly independent $f_1,\cdots,f_b$ in $A'_q(\Sigma,\mathfrak{U}^\dagger)$, the set of elements $E^\dagger$ in $\mathfrak{U}^\dagger$ such that $\kappa_{E^\dagger}(f_1),\cdots,\kappa_{E^\dagger}(f_b)$ are linearly dependent forms a proper subvariety of $\mathfrak{U}^\dagger$. It is also clear that there are homogeneous elements $f_1,\cdots,f_b$ in $A'_q(\Sigma,\mathfrak{U}^\dagger)$ such that they $[\Lambda^0]\mathfrak{U}^\dagger$-generate $A^{[l+1]}{}_q(\Sigma,\mathfrak{U}^\dagger)$ and such that, for any $E^\dagger$ in $\mathfrak{U}^\dagger$, $\kappa_{E^\dagger}(f_1),\cdots,\kappa_{E^\dagger}(f_b)$ generate $A^{l+1}{}_q(\Sigma,E^\dagger)$. Then Propositions III. 8 (i) and (iii) imply that $E^\dagger$ is in $S(\Sigma,\Omega,l;q) \cap \mathfrak{U}^\dagger$ if and only if, for any subset $f_{i_1},\cdots,f_{i_a}$ which is a base of $A^{[l+1]}{}_q(\Sigma,\mathfrak{U}^\dagger)$, $\kappa_{E^\dagger}(f_{i_1}),\cdots,\kappa_{E^\dagger}(f_{i_a})$ are linearly dependent. Therefore $S(\Sigma,\Omega,l;q) \cap \mathfrak{U}^\dagger$ is a proper subvariety of $\mathfrak{U}^\dagger$.

LEMMA III. 4. *Let $S^\dagger$ be an element of $\mathfrak{G}^\dagger(\mathfrak{V},q)$ such that, for an integer l, $\phi^l{}_q(\Sigma,\Omega) = \phi^l(\Sigma,E^\dagger)$. Assume that $l \geqq l_0(\Sigma,\Omega)$. Then $\phi^{l+1}{}_q(\Sigma,\Omega) = \phi^{l+1}(\Sigma,E^\dagger)$.*

Proof. Let $\omega^1,\cdots,\omega^p$ be a base of Ω such that $\langle\omega^1,E^\dagger\rangle,\cdots,\langle\omega^q,E^\dagger\rangle$ are linearly independent. Set $\mathfrak{U}^\dagger = \mathfrak{U}^\dagger(\omega^1,\cdots,\omega^q)$. Then

$$
\begin{aligned}
\phi^{l+1}{}_q(\Sigma,\Omega) &= \phi^{l+1}(A_q(\Sigma,\mathfrak{U}^\dagger)), && \text{(by Prop. III. 7)},\\
&= Q(\phi^l(A_q(\Sigma,\mathfrak{U}^\dagger)),p+m), && \text{(by Theorem III. 1)},\\
&= Q(\phi^l(A(E^\dagger)),p+m), && \text{(by the assumption)},\\
&\leqq \phi^{l+1}(A(E^\dagger)). && \text{(by Theorem III. 1)},\\
&= \phi^{l+1}(\Sigma,E^\dagger), && \text{(by Def. III. 3)}.
\end{aligned}
$$

Therefore, Proposition III. 8(i) implies that $\phi^{l+1}{}_q(\Sigma,\Omega) = \phi^{l+1}(\Sigma,E^\dagger)$.

By Lemma III. 4 it follows that the sequence $S(\Sigma, \Omega, l)$ for $l \geqq l_0(\Sigma, \Omega)$ is decreasing. Hence

$$(66)' \qquad S(\Sigma, \Omega) = \bigcap_l S(\Sigma, \Omega, l).$$

Proof of Theorem 2. Take $\omega^1, \cdots, \omega^p$ and $\varpi^1, \cdots, \varpi^m$ as in Proposition III. 5. Denote tentatively by ρ the projection $\mathfrak{G}^\dagger(\mathfrak{V}, q) \to \mathfrak{V}$. Set $\mathfrak{U}^\dagger = \mathfrak{U}(\omega^1, \cdots, \omega^q)$. Define the function ${}^q w_r{}^h$ by the formula (46). Let $\mathfrak{N}_\epsilon{}^\dagger$ be the set of all $E^\dagger$ in $\mathfrak{U}^\dagger$ such that $|{}^q w_r{}^h(E^\dagger)| < \epsilon$ for any $r = 1, \cdots, q$ and $h = 1, \cdots, p - q$. Now there does not exist $E^\dagger$ in $\rho^{-1}(x)$ such that $\phi^{l+1}{}_q(\Sigma, \Omega) = \phi^{l+1}(\Sigma, E^\dagger)$ if and only if $\rho^{-1}(x) \subseteq S(\Sigma, \Omega, l; q)$. Since $\rho^{-1}(x)$ is a connected submanifold of $\mathfrak{G}^\dagger(\mathfrak{V}, q)$ and $S(\Sigma, \Omega, l; q)$ is a subvariety of $\mathfrak{G}^\dagger(\mathfrak{V}, q)$, either $\rho^{-1}(x) \cap S(\Sigma, \Omega, l, q) = \rho^{-1}(x)$ or $\rho^{-1}(x) \cap S(\Sigma, \Omega, l, q)$ does not contain any non empty open subset of $\rho^{-1}(x)$. Therefore it follows that there does not exist $E^\dagger$ in $\rho^{-1}(x)$ such that $\phi^{l+1}{}_q(\Sigma, \Omega) = \phi^{l+1}(\Sigma, E^\dagger)$ if and only if $\rho^{-1}(x) \cap \mathfrak{N}_\epsilon{}^\dagger \subseteq S(\Sigma, \Omega, l; q)$, because $\rho^{-1}(x) \cap \mathfrak{N}_\epsilon{}^\dagger$ is a non empty open subset of $\rho^{-1}(x)$.

Fix a point x in $\mathfrak{V}$. Take an open neighborhood N of x and ϵ so small that $S(\Sigma, \Omega, l; q) \cap \rho^{-1}(N) \cap \mathfrak{N}_\epsilon{}^\dagger$ is equal to the set of common zeros of functions $f_\mu(x, w)$ on $\rho^{-1}(N) \cap \mathfrak{N}_\epsilon{}^\dagger$. For any system of values $a \equiv (a_r{}^h)$, $(|a_r{}^h| < \epsilon)$, denote by $f_\mu{}^a(x) = f_\mu(x, \cdots a_r{}^h \cdots)$. Denote by $S^l{}_q$ the set of all x' in $\mathfrak{V}$ such that there does not exist $E^\dagger$ in $\rho^{-1}(x)$ such that $\phi^{l+1}{}_q(\Sigma, \Omega) = \phi^{l+1}(\Sigma, E^\dagger)$. Then the conclusion reached above implies that $S^l{}_q \cap N$ is equal to the common zeros of all $f_\mu{}^a$, that is, $S^l{}_q$ is a proper subvariety. Therefore $S(\Sigma, \Omega, l) = \bigcup \{S^l{}_q; q = 0, 1, \cdots, q - 1\}$ is a proper subvariety. By (66)$'$, $S(\Sigma, \Omega)$ is also a subvariety.

Theorem III. 3 follows easily from Lemma III. 4. Theorem III. 4 follows easily from Theorem III. 2 and Lemma III. 4.

5. Regular bases. Let $L^\dagger$ be a reduced tangent vector to $\mathfrak{V}$ at x. We remark that $P^{[0,1]}(x) = \mathfrak{E}^\dagger{}_x\mathfrak{V} \ni L^\dagger$ (cf. (55)) and so the product $v \cdot L^\dagger$ is defined for any $v \in P(x)$. Let $E^\dagger$, x as its origin, be an element in $\mathfrak{G}^\dagger(\mathfrak{V}, q)$.

Definition III. 6. $L^\dagger$ is called l_1-prime to $E^\dagger$ (with respect to (Σ, Ω)) if the conditions $v \in P^{[1,l]}(x)$, $l \geqq l_1$, and $v \cdot L^\dagger \in A(E^\dagger)$ always imply that v is in $A(E^\dagger)$.

LEMMA III. 5. *Let $E^\dagger$ be an element in $\mathfrak{G}^\dagger(\mathfrak{V}, q)$ $(q = 0, 1, \cdots, p - 1)$. Then there is an integer $l_1 = l_1(E^\dagger)$ such that the set of reduced tangent*

vectors $L^\dagger$ at the origin x of $E^\dagger$ which are l_1-prime to $E^\dagger$ is everywhere dense in $\mathcal{E}^\dagger{}_x\mathfrak{V}$.

Proof. Since $P(x)$ is a Noetherian ring, $A(E^\dagger) = \mathfrak{Q}_1 \cap \cdots \cap \mathfrak{Q}_a$, where $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_a$ are primary ideals of $P(x)$. It is well known that $\mathfrak{P}_\nu = \{v \in P(x)$; there is an integer τ such that $v^\tau \in \mathfrak{Q}_\nu\}$ is a prime ideal of $P(x)$. There is an integer μ_ν such that $\mathfrak{P}_\nu{}^{\mu_\nu} \subseteq \mathfrak{Q}_\nu$ $(\nu = 1, \cdots, a)$. We can assume that, for $\nu = 1, \cdots, b$ $(b \leqq a)$, and for any integer l, $\mathfrak{Q}_\nu$ *does* not contain $P^{[1,l]}(x)$, but that, for each $\nu = b+1, \cdots, a$, there is an integer $l(\nu)$ such that $\mathfrak{Q}_\nu \supseteq P^{[1,l]}(x)$ for any $l > l(\nu)$. b may be equal to zero. In this case $A^{[1,l]}(E^\dagger) = P^{[1,l]}(x)$ for $l \geqq l_1 = \mathrm{Max}\{l(\nu)\,; \nu = 1, \cdots, a\}$. Therefore any vector $L^\dagger$ in $\mathcal{E}^\dagger{}_x\mathfrak{V}$ is l_1-prime to $E^\dagger$. Hence we shall suppose that $b > 0$. Put $l_1 = \mathrm{Max}\{l(\nu)\,; \nu = b+1, \cdots, a\}$ if $b < a$, and $l_1 = 1$ if $b = a$. Set $A = \mathfrak{Q}_1 \cap \cdots \mathfrak{Q}_b$. Then

$$A \cap P^{[1,l]}(x) = A^{[1,l]}(E^\dagger) \quad \text{for } l \geqq l_1. \tag{67}$$

The choice of b and the property $\mathfrak{P}_\nu{}^{\mu_\nu} \subseteq \mathfrak{Q}_\nu$ imply that $\mathfrak{P}_\nu \cap P^{[0,1]}(x)$ is a proper subspace of $\mathcal{E}^\dagger{}_x\mathfrak{V} = P^{[0,1]}(x)$ for $\nu = 1, \cdots, b$. Assume that $L^\dagger \notin (\mathfrak{P}_1 \cup \cdots \cup \mathfrak{P}_b) \cap P^{[0,1]}(x)$. Let v be an element of $P^{[1,l]}(x)$, where $l \geqq l_1$, such that $v \cdot L^\dagger \in A(E^\dagger)$. Then, for $\nu = 1, \cdots, b$, $v \cdot L^\dagger \in \mathfrak{Q}_\nu$ and $L^\dagger \notin \mathfrak{P}_\nu$. Hence $v \in \mathfrak{Q}_\nu$, i.e., $v \in A = \mathfrak{Q}_1 \cap \cdots \mathfrak{Q}_b$. Then (67) implies that $v \in A(E^\dagger)$. Thus the complementary set of $(\mathfrak{P}_1 \cup \cdots \cup \mathfrak{P}_b) \cap \mathcal{E}^\dagger{}_x\mathfrak{V}$, which is everywhere dense, consists of vectors l_1-prime to $E^\dagger$.

Definition III. 7. Let $\omega^1, \cdots, \omega^p$ be an ordered base of Ω. Let x be a point in $\mathfrak{V}$. By a dual reduced flag at x to the ordered base $\omega^1, \cdots, \omega^p$ we mean the flag $F^\dagger$ on $\mathcal{E}^\dagger{}_x\mathfrak{V}$ such that the q-th component $E_q{}^\dagger$ of $F^\dagger$ satisfies the conditions: $\langle \omega^{q+1}, E_q{}^\dagger \rangle = \cdots = \langle \omega^p, E_q{}^\dagger \rangle = 0$ for $q = 0, 1, \cdots, p-1$ (cf. Definition III. 5).

Thus for each ordered base $\omega^1, \cdots, \omega^p$ of Ω, there is one and only one dual reduced flag at x to $\omega^1, \cdots, \omega^p$. Conversely, any reduced flag is the dual reduced flag of an ordered base, since for any base of Ω, the linear transformation of it by non-singular matrix with constant coefficients is again a base of Ω (note that $d\omega^i = 0$).

Definition III. 8. An ordered base $\omega^1, \cdots, \omega^p$ of Ω is called l_1-regular at x (with respect to (Σ, Ω)), if it satisfies the following conditions:

(i) the dual reduced flag ${}^0F^\dagger$ at x to $\omega^1, \cdots, \omega^p$ is a regular reduced flag at x of weight l_1;

(ii) $X_i = L_i(\mathcal{E}^{\dagger}{}_x\mathcal{V})$ (cf. $(6)^{\dagger}$ for $q=p$, $i=1,\cdots,p$), is l_1-prime to ${}^oE_{i-1}{}^{\dagger}$ for $i=1,\cdots,p$, where ${}^oE_i{}^{\dagger}$ is the i-th component of the reduced flag ${}^oF^{\dagger}$.

THEOREM III.5. *Let (Σ,Ω) be a normal system. Let x be a $\mathcal{P}$-regular point of weight l_0. Then there is an ordered base $\omega^1,\cdots,\omega^p$ of Ω which is l_1-regular at x for sufficiently large l_1.*

Proof. If x is a $\mathcal{P}$-regular point of weight l_0, then x is a $\mathcal{P}$-regular point of weight l for any $l \geqq l_0$. Therefore we can assume that $l_0 \geqq l_0(\Sigma,\Omega)$. Take a regular flag $F^{\dagger}$ of weight l_0 at x (Theorem III.4). Let $E_q{}^{\dagger}$ be the q-th component of $F^{\dagger}$. Then there is a neighborhood $\mathfrak{N}_q$ of $E_q{}^{\dagger}$ in the manifold of all q dimensional subspaces of $\mathcal{E}^{\dagger}{}_x\mathcal{V}$ such that any reduced flag $'F^{\dagger}$, of which q-th component is in $\mathfrak{N}_q$ for $q=1,\cdots,p-1$, is again a reduced regular flag at x of weight l_0 (cf. Theorem III.4). Let us choose $\mathfrak{N}_q$ in such a way that, for any $'E_q{}^{\dagger}$ in $\mathfrak{N}_q$, the set of all vectors $L^{\dagger}$ in $\mathcal{E}^{\dagger}{}_x\mathcal{V}$ such that the space spanned by $'E_q{}^{\dagger}$ and $L^{\dagger}$ is in $\mathfrak{N}_{q+1}$ contains an interior point for $q=0,\cdots,p-2$. Set ${}^oE_0{}^{\dagger}=\{x\}$. Then, by Lemma III.5, there is a vector $L_1{}^{\dagger}$ in $\mathcal{E}^{\dagger}{}_x\mathcal{V}$ which is l^0-prime to ${}^oE_0{}^{\dagger}$ and the space ${}^oE_1{}^{\dagger}$ spanned by $L_1{}^{\dagger}$ and ${}^oE_0{}^{\dagger}$ is in $\mathfrak{N}_1$, where $l^0 = l_1({}^oE_0{}^{\dagger})$ (cf. Lemma III.5). Continuing this process, we can choose easily ${}^oE_q{}^{\dagger}$ in $\mathfrak{N}_q$ and $L_{q+1}{}^{\dagger}$ in $\mathcal{E}^{\dagger}{}_x\mathcal{V}$ $(q=0,1,\cdots,p-1)$ such that $\{{}^oE_q{}^{\dagger}\}$ form a reduced flag at x, ${}^oE_{q+1}{}^{\dagger}$ is generated by ${}^oE_q{}^{\dagger}$ and by $L_{q+1}{}^{\dagger}$, and such that $L_{q+1}{}^{\dagger}$ is l^q-prime to ${}^oE_q{}^{\dagger}$, where $l^q = l_1({}^oE_q{}^{\dagger})$. Set $l_1 = \mathrm{Max}\{l^0,\cdots,l^{q-1}\}$. Then it is easy to see that an ordered base of Ω such that ${}^oF^{\dagger}$ is the dual reduced flag to the base is l_1-regular at x, since if X is l-prime to ${}^oE_q{}^{\dagger}$ then any vector in the space spanned by X and ${}^oE_q{}^{\dagger}$ but not in ${}^oE_q{}^{\dagger}$ is again l-prime to ${}^oE_q{}^{\dagger}$.

THEOREM III.6. *Let (Σ,Ω) be a normal system with p independent variables. Then there is an integer $l_1(\Sigma,\Omega)$ such that for $l \geqq l_1(\Sigma,\Omega)$*

$$t^l{}_q(\Sigma,\Omega) = n_{l-1} - t^{l-1}{}_{q-1}(\Sigma,\Omega) + t^l{}_{q-1}(\Sigma,\Omega)$$

where $1 \leqq q \leqq p$ and $n_l = mC_l{}^{p+l-1}$.

Proof. By Theorem III.2 there is a $\mathcal{P}$-regular point x of weight l_0. By Theorem III.5, there is an ordered base $\omega^1,\cdots,\omega^p$ of Ω which is l_1-regular at x. Let $F^{\dagger}$ be the dual reduced flag at x to $\omega^1,\cdots,\omega^p$. Let $E_q{}^{\dagger}$ $(q=0,1,\cdots,p)$ be the q-th component of $F^{\dagger}$. Then $\phi^l{}_q(\Sigma,\Omega) = \phi^l(\Sigma,E_q{}^{\dagger})$ for $l \geqq l_1$. Hence by Definition III.3, Proposition III.8 (ii),

$$t^l{}_q(\Sigma,\Omega) = t^l(\Sigma,E_q{}^{\dagger}) \qquad (l \geqq l_1 - 1). \tag{68}$$

Let $X_1,\cdots,X_p$ be the base in $\mathcal{E}^\dagger_x\mathfrak{V}$ dual to $\langle\omega^1,\mathcal{E}^\dagger_x\mathfrak{V}\rangle,\cdots,\langle\omega^p,\mathcal{E}^\dagger_x\mathfrak{V}\rangle$. Then $E_q{}^\dagger$ is generated by $X_1,\cdots,X_q$. By Proposition III. 6, $A(E_q{}^\dagger)^{[1,l]}$ is generated as a vector space by all

$$\xi_{\phi;ij}(E_q{}^\dagger)\cdot X_{k_1}\cdots X_{k_{l-1}} \text{ and } \zeta^\lambda{}_r(E_q{}^\dagger)\cdot X_{k_1}\cdots X_{k_{l-1}}$$

$$(\phi\in\Sigma^{[2]};i,j,k_1,\cdots,k_{l-1}=1,\cdots,p;\lambda=1,\cdots,m;r=1,\cdots,q),$$

for each q. Therefore since $\xi_{\phi;ij}(E_q)^\dagger=\xi_{\phi;ij}(E_{q-1}{}^\dagger)$ and $\xi^\lambda{}_{r'}(E_q{}^\dagger)=\xi^\lambda{}_{r'}(E_{q-1}{}^\dagger)$ for $r'=1,\cdots,q-1$,

$$A(E_q{}^\dagger)^{[1,l]}=A(E_{q-1}{}^\dagger)^{[1,l]}+\sum_{\lambda=1}^{m}\xi^\lambda{}_q(E_q{}^\dagger)P^{[0,l-1]}(x)$$

for $q\geqq 1$. On the other hand ${}^qw_q{}^h(E_q{}^\dagger)=0$ for $h=1,\cdots,p-q$, since $F^\dagger$ is the dual reduced flag at x to $\omega^1,\cdots,\omega^p$. Hence, by (58)′, $\xi^\lambda{}_q(E_q{}^\dagger)=Y^\lambda X_q$. Then, for $q\geqq 1$,

$$A(E_q{}^\dagger)^{[1,l]}=A(E_{q-1}{}^\dagger)^{[1,l]}+X_qP^{[1,l-1]}(x),$$

since $P^{[1,l-1]}(x)=Y^1P^{[0,l-1]}(x)+\cdots+Y^mP^{[0,l-1]}(x)$. Let $v_1,\cdots,v_a$ be a base of $P^{[1,l-1]}(x)$ modulo $A(E_{q-1}{}^\dagger)^{[1,l-1]}$. Then

$$A(E_q{}^\dagger)^{[1,l]}=A(E_{q-1}{}^\dagger)^{[1,l]}+X_q\cdot\boldsymbol{R}v_1+\cdots+X_q\cdot\boldsymbol{R}v_a.$$

Since $\omega^1,\cdots,\omega^p$ is l_1-regular, X_q is l_1-prime to $A(E_{q-1}{}^\dagger)$. Therefore it follows that the above sum is a direct sum, that is,

$$t^l(\Sigma,E_q)=\dim(A(E_q{}^\dagger)^{[1,l]})=t^l(\Sigma,E_{q-1}{}^\dagger)+a.$$

By the definition of a, $a=n_{l-1}-t^{l-1}(\Sigma,E_{q-1})$. Hence

$$(69)\qquad t^l(\Sigma,E_q{}^\dagger)=n_{l-1}-t^{l-1}(\Sigma,E_{q-1}{}^\dagger)+t^l(\Sigma,E_{q-1}{}^\dagger)\qquad(l\geqq l_1)$$

Then the theorem follows from (68) and (69).

6. The fundamental theorem. Let (Σ',Ω') be an exterior differential system with independent variables on a real analytic manifold $\mathfrak{V}'$.

Definition III. 9. An integral point y of (Σ',Ω') is called normal if y is an ordinary integral point and if there is a neighborhood $\mathfrak{N}$ of y in $\mathfrak{V}'$ such that for any y' in $\mathfrak{N}\cap\mathfrak{J}^0\Sigma'$

$$(70)\qquad \langle\Sigma'^{[1]}\cap\Omega',\mathcal{E}_{y'}\mathfrak{V}'\rangle=0.$$

Proposition III. 9. If (Σ',Ω') is involutive at an integral point y. then y is normal.

Proof. By Definition I. 17, y must be an ordinary integral point and there is a p dimensional integral element E of (Σ', Ω') at y such that $\langle \Omega', E \rangle$ is p dimensional, where p is the number of independent variables in Ω'. Let $\omega^1, \cdots, \omega^p$ be a base of Ω'. By Proposition I. 6, there is a neighborhood $\mathfrak{N}$ of y in $\mathfrak{V}'$ such that, for any y' in $\mathfrak{N} \cap \mathfrak{J}^0\Sigma'$, there is an an integral element E' on which $\omega^1, \cdots, \omega^p$ are linearly independent. Take an element $a_1\langle \omega^1, \mathcal{E}_{y'}\mathfrak{V}' \rangle + \cdots + a_p\langle \omega^p, \mathcal{E}_{y'}\mathfrak{V}' \rangle \in \langle \Sigma' \cap \Omega', \mathcal{E}_{y'}\mathfrak{V}' \rangle$. Since $\langle \Sigma'^{[1]} \cap E' \rangle = 0$, $\langle a_1\omega^1 + \cdots + a_p\omega^p, E' \rangle = 0$, that is $a_1 = \cdots = a_p = 0$. Therefore y is a normal point.

THEOREM III.7. *Let (Σ, Ω) be a normal system on $\mathfrak{V}$. Let x be a $\mathfrak{P}$-regular point iwth respect to (Σ, Ω). Let $\omega^1, \cdots, \omega^p$ be an ordered base of Ω which is l_1-regular. Construct $(\mathfrak{R}_l\Sigma, \Omega)$ by the base $\omega^1, \cdots, \omega^p$. Let y be an integral point of $(\mathfrak{R}_l\Sigma, \Omega)$. Assume that $l \geqq l_1$ and that $\rho_0{}^l(y) = x$, where $\rho_0{}^l$ is the projection of $\mathfrak{R}$ onto $\mathfrak{V} = \mathfrak{R}_0$. Then $(\mathfrak{R}_l\Sigma, \Omega)$ is involutive at y if and only if y is a normal point of $(\mathfrak{R}_l\Sigma, \Omega)$. Moreover if y is normal, and if E is p-dimensional integral element of $(\mathfrak{R}_l\Sigma, \Omega)$ at y, then the system of characters of E is given by the following formula:*

$$s_0(E) = t^l{}_0(\Sigma, \Omega) + n - p + m\Big(\sum_{\nu=1}^{l-1} C_\nu{}^{p+\nu-1}\Big);$$

$$s_q(E) = t^l{}_q(\Sigma, \Omega) - t^l{}_{q-1}(\Sigma, \Omega) \text{ for } q = 1, \cdots, p-1,$$

where p is the number of independent variables in Ω.

Proof. By Proposition III. 9, it is sufficient to show that, if y is normal, then $(\mathfrak{R}_l\Sigma, \Omega)$ is involutive at y. Let $\mathfrak{N}_l$ be a neighborhood of y such that, for any $y' \in \mathfrak{N}_l \cap \mathfrak{J}^0\mathfrak{R}_l\Sigma$,

$$\langle \mathfrak{R}_l\Sigma^{[1]} \cap \Omega, \mathcal{E}_{y'}\mathfrak{R}_l \rangle = 0. \tag{71}$$

Let $F^\dagger$ be the dual reduced flag at x to $\omega^1, \cdots, \omega^p$. Denote by $E_q{}^\dagger$ the q-th component of $F^\dagger$. Then there is a neighborhood $\mathfrak{N}_q{}^\dagger$ of $E_q{}^\dagger$ in $\mathfrak{G}^\dagger(\mathfrak{V}, q)$ such that, for any $E^\dagger$ in $\mathfrak{N}_q{}^\dagger$, we have the equality

$$t^l{}_q(\Sigma, \Omega) = t^l(\Sigma, E^\dagger), \tag{72}$$

because $\omega^1, \cdots, \omega^p$ is a l_1-regular base (cf. Lemma III. 3 and Lemma III. 4. We can choose $\mathfrak{N}_q{}^\dagger$ in such a way that $\rho_0{}^l(\mathfrak{N}_l) \supseteq \mathfrak{N}_0{}^\dagger$ and such that $\eta^\dagger{}_q(\mathfrak{N}^\dagger{}_q) \subseteq \mathfrak{N}^\dagger{}_{q-1}$ (cf. (47)). First we maintain the following, for $q = 0, 1, \cdots, p-1$.

$(*)_q$: Let E be a q-dimensional integral element of $(\mathcal{R}_l\Sigma, \Omega)$ such that $\mu(E)$ (cf. (61)), is in $\mathfrak{N}^\dagger_q$ and such that its origin is in $\mathfrak{N}_l$. Then

$$\dim J(E) = \dim (J(E) \bmod \langle \Omega, \mathcal{E}_{y'}\mathcal{R}_l\rangle)$$
$$= t^l_q(\Sigma, \Omega) + n - p + m(\sum_{\nu=1}^{l-1} C_\nu^{p+\nu-1}),$$

where y' is the origin of E. By Proposition II. 4, (45), and (45)$'$,

$$\dim (J(E) \bmod \langle \Omega, \mathcal{E}_{y'}\mathcal{R}_l\rangle) = t'(E) + n - p + m(\sum_{\nu=1}^{l-1} (C_\nu^{p+\nu-1}))$$
$$\leqq \dim (\langle A_l^q, \mathcal{E}_{y'}\mathcal{R}_l\rangle_E) + n - p + m(\sum_{\nu=1}^{l-1} (C_\nu^{p+\nu-1})) = \dim (J(E)).$$

Therefore, by (62) and (72), it is sufficient to show that

$$(73)_q \qquad \dim \langle A_l^q, \mathcal{E}_{y'}\mathcal{R}_l\rangle_E = t^l_q(\Sigma, \Omega).$$

We shall prove this equality by induction on q. Let y' be an integral point in $\mathfrak{N}_0$. Then, since $\langle A_l^0, \mathcal{E}_{y'}\mathcal{R}_l\rangle \subseteq \langle \mathcal{R}_l\Sigma^{[1]}, \mathcal{E}_{y'}\mathcal{R}_l\rangle$, (71) implies that $\dim \langle A_l^0, \mathcal{E}_{y'}\mathcal{R}_l\rangle = \dim \langle A'^0_l, \mathcal{E}_{y'}\mathcal{R}_l\rangle = t^l_0(\Sigma, y') = t^l_0(\Sigma, \Omega)$. Assume that $(73)_{q-1}$ is proved and that E is a q-dimensional integral element of $\mathcal{R}_l\Sigma$ such that $\mu(E) \in \mathfrak{N}_q^\dagger$. Then $E' = \eta_q(E)$ is a $q-1$-dimensional integral element of $\mathcal{R}_l\Sigma$ such that $\mu(E') \in \mathfrak{N}_{q-1}^\dagger$. Hence by Proposition II. 6, (45), (62), (72), and $(73)_{q-1}$,

$$t^l_q(\Sigma, \Omega) \leqq \dim \langle A_l^q, \mathcal{E}_{y'}\mathcal{R}_l\rangle_E \leqq t^l_{q-1}(\Sigma, \Omega) + n_{l-1} - t^{l-1}_{q-1}(\Sigma, \Omega),$$

since $\mu(d\rho_{l-1}{}^lE') = \mu(E')$. Then Theorem III. 6 implies the equality $(73)_q$. Therefore we have proved $(*)_q$ for $q = 0, 1, \cdots, p-1$.

Now let E be a p dimensional integral element of $(\mathcal{R}_l\Sigma, \Omega)$. Then there is a unique subspace E_q of E such that $\mu(E_q) = E_q^\dagger$ for $q = 0, 1, \cdots, p$. The spaces E_q form a flag on E. Let $\mathfrak{N}_{l,q}$ be a neighborhood of E_q such that $\rho(\mathfrak{N}_{l,q}) \subseteq \mathfrak{N}_l$ and $\mu(\mathfrak{N}_{l,q}) \subseteq \mathfrak{N}_q^\dagger$. Then for any $E \in \mathfrak{N}_{l,q} \cap \mathfrak{I}^q\mathcal{R}_l\Sigma$,

$$\dim J(E) = t^l_q(\Sigma, \Omega) + n - p + m(\sum_{\nu=0}^{l-1} C_\nu^{p+\nu-1})$$

for $q = 0, 1, \cdots, p-1$. This shows that, on a neighborhood of E_q in $\mathfrak{I}^q\mathcal{R}_l\Sigma$, the rank of system of polar forms remains constant, for $q = 0, 1, \cdots, p-1$. Therefore E is an ordinary integral element. Moreover we have the formulas:

$$s_0(E) = t^l_0(\Sigma, \Omega) + n - p + m(\sum_{\nu=1}^{l-1} C_\nu^{p+\nu-1});$$
$$s_q(E) = t^l_q(\Sigma, \Omega) - t^l_{q-1}(\Sigma, \Omega) \text{ for } p-1 \geqq q \geqq 1;$$
$$s_p(E) = mC_l^{p+l-1} - t^l_{p-1}(\Sigma, \Omega).$$

We must show that there is at least one q dimensional integral element E of origin y. By $(*)_0$, we know that $\dim J(y) = \dim(J(y) \bmod \langle \Omega, \mathcal{E}_y \mathcal{R}_l \rangle)$. Therefore we can solve the equation $J(y) = 0$, under the conditions:

$$\langle \omega^1, \mathcal{E}_y \mathcal{R}_l \rangle = 1, \langle \omega^2, \mathcal{E}_y \mathcal{R}_l \rangle = \cdot\ \cdot\ \cdot = \langle \omega^p, \mathcal{E}_y \mathcal{R}_l \rangle = 0.$$

Let L_1 be a solution. Let E_1 be the 1-dimensional contact element spanned by L_1. Then E_1 is 1-dimensional integral element of $\mathcal{R}_l \Sigma$ such that $\mu(E_1) = E_1{}^{\dagger}$. Then, since $\dim J(E_1) = \dim(J(E_1) \text{ modulo } \langle \Omega, \mathcal{E}_y \mathcal{R}_l \rangle)$ by $(*)_1$, there is a tangent vector L_2 to $\mathcal{R}_l$ at y such that $\langle J(E_1), L_2 \rangle = 0$, $\langle \omega^2, L_2 \rangle = 1$, $\langle \omega^1, L_2 \rangle = \langle \omega^3, L_2 \rangle = \cdot\ \cdot\ \cdot = \langle \omega^p, L_2 \rangle = 0$. Then the contact element E_2 spanned by E_1 and L_2 is an integral element such that $\mu(E_2) = E_2{}^{\dagger}$. Repeating this process, we can obtain a p dimensional integral element E at y on which $\omega^1, \cdot\ \cdot\ \cdot, \omega^p$ are linearly independent. Therefore $(\mathcal{R}_l \Sigma, \Omega)$ is involutive at y.

FUNDAMENTAL THEOREM. *Let (Σ, Ω) be a normal system with p independent variable on $\mathfrak{V}$. Let $\mathfrak{P}^l(\Sigma, \Omega)$ be the l-th prolongation of (Σ, Ω). $\mathfrak{P}^l(\Sigma, \Omega)$ is defined on $\mathfrak{G}^l(\mathfrak{V}, p) = \mathfrak{V}_l$. Let ρ^l be the natural projection of $\mathfrak{V}_l$ onto $\mathfrak{V}$. Let x be a $\mathfrak{P}$-regular point of (Σ, Ω). Then there is an integer $l_1(x)$ satisfying the following conditions: if y is an integral point of $\mathfrak{P}^l(\Sigma, \Omega)$ and if $l \geqq l_1(x)$ then $\mathfrak{P}^l(\Sigma, \Omega)$ is involutive at y if and only if y is a normal point of $\mathfrak{P}^l(\Sigma, \Omega)$. In this case the sytem of characters of a p-dimensional integral element E at y is given by the following formula*

$$s_0(E) = t^l{}_0(\Sigma, \Omega) + n - p + m\left(\sum_{\nu=1}^{l-1} (C_\nu{}^{p+\nu-1})\right) + c_l;$$

$$s_q(E) = t^l{}_q(\Sigma, \Omega) - t^l{}_{q-1}(\Sigma, \Omega) \text{ for } q = 0, 1, \cdot\ \cdot\ \cdot, p-1;$$

$$s_p(E) = mC_l{}^{p+l-1} - t^l{}_{p-1}(\Sigma, \Omega).$$

where $c_l = \sum_{\nu=0}^{l-1} (p+1)^{l-1-\nu} c'_l$, $c'_0 = \alpha_1 p$,

$$c'_\nu = \alpha\, p + mp\,\tfrac{1}{2}(p-1)(C_{\nu-1}{}^{p+\nu-2}) + \sum_{h=1}^{\nu-1} (C_h{}^{p+h-1})$$

for $\nu \geqq 1$, and α_1 is the maximal number of linearly independent Pfaffian forms in $\Sigma^{[1]}$.

Proof. By Theorem III. 5, there is an ordered base $\omega^1, \cdot\ \cdot\ \cdot, \omega^p$ of Ω which is l_1-regular at x. Set $l_1(x) = l_1$. Then the theorem follows easily from Theorem II. 2, Theorem III. 7, and from Proposition II. 1.

7. An example. If one replaces the condition (70) by the following weaker condition:

$$\langle d(\Sigma')^{[0]} \cap \Omega', \mathcal{E}_y'\mathcal{V}'\rangle = 0 \tag{74}$$

then the Fundamental theorem does not hold for this definition of normal point, that is, (70) does not imply (74), as one can see easily by the following.

Example 2. Let $\mathcal{V}$ be a 4-dimensional euclidean space with a system of coordinates (x_1, x_2, u^1, u^2). Set $\omega^1 = dx_1$, $\omega^2 = dx_2$, $\varpi^1 = du^1$, and $\varpi^2 = du^2$. Let Ω be the system of 2 independent variables generated by ω^1 and ω^2. Let Σ be the exterior differential system generated by

$$\phi_{(1)} = x_2\omega^1 \wedge \varpi^1 + u^1\omega^1 \wedge \omega^2;$$

$$\phi_{(2)} = -x_1\omega^2 \wedge \varpi^2 + u^2\omega^1 \wedge \omega^2;$$

$$\phi_{(3)} = \omega^1 \wedge \varpi^1 + \omega^2 \wedge \varpi^2.$$

Clearly the subspace: $u^1 = u^2 = 0$ is an integral manifold of (Σ, Ω). We shall show that (i) there exists a $\mathfrak{P}$-regular point P such that $u^1(P) = u^2(P) = 0$, $x^1(P) \neq 0$, $x^2(P) \neq 0$, (ii) if y is any integral point of $\mathfrak{P}^l(\Sigma, \Omega)$ such that $\rho^l(y) = P$, y is an ordinary integral point and satisfies (74) but not (70).

By Theorem II.2, it is sufficient to observe $(\mathcal{R}_l\Sigma, \Omega)$. It is easy to see that

$$\Theta_{(1)12;} = x_2u^1{}_2 + u^1; \quad \Theta_{(2)12;} = x_1u^2{}_1 + u^2; \quad \Theta_{(3)12;} = u^1{}_2 - u^2{}_1, \cdots,$$

$$\Theta_{(1)12;k_1\cdots k_l} = x_2u^1{}_{2k_1\cdots k_l} + (1 + \sum_{\nu=1}^{l} \delta_{k_\nu}{}^2)u^1{}_{k_1\cdots k_l};$$

$$\Theta_{(2)12;k_1\cdots k_l} = x_1u^2{}_{1k_1\cdots k_l} + (1 + \sum_{\nu=1}^{l} \delta_{k_\nu}{}^1)u^2{}_{k_1\cdots k_l};$$

$$\Theta_{(3)12;k_1\cdots k_l} = u^1{}_{2k_1\cdots k_l} - u^2{}_{1k_1\cdots k_l}.$$

Thus the coefficients of elements in $(A'_l{}^q)$, when they are written by power series of x_1, x_2, u^1, u^2, do not contain u^1 and u^2. Hence if P' is a $\mathfrak{P}$-regular point, then the point P such that $x^1(P) = x^1(P')$, $x^2(P) = x^2(P')$, $u^1(P) = u^2(P) = 0$, is also a $\mathfrak{P}$-regular point. Moreover, it is clear that there is a $\mathfrak{P}$-regular point P' such that $x^1(P') \neq 0$ and $x^2(P') \neq 0$ (Theorem III.2). This proves (i). Set

$$\epsilon(k_1, \cdots, k_l) = (-1)^{l+1} \prod_{\nu=1}^{l-1} (1 + \sum_{\mu=\nu+1}^{l} \delta_{k_\mu}{}^{k_\nu}), \quad (l \geqq 2).$$

Then it is easy to see that $\epsilon(k_1,\cdots,k_l)=\epsilon(k_{\pi(1)}\cdots k_{\pi(l)})$ for any permutation π of l letters, and that

$$\epsilon(1,2,k_1,\cdots,k_l)=-(1+\sum_{\nu=1}^{l}\delta_{k_\nu}{}^2)\cdot\epsilon(1,k_1,\cdots,k_l)$$
$$=-(1+\sum_{\nu=1}^{l}\delta_{k_\nu}{}^1)\cdot\epsilon(2,k_1,\cdots,k_l).$$

Now $\mathfrak{R}_l$ is a euclidean space of dimensions $4+2\sum_{\nu=1}^{l}(\nu+1)$, with the system of coordinates

$$(x_1,x_2,u^1,u^2,\cdots,u^\lambda{}_{k_1\cdots k_\nu},\cdots),\qquad(\nu=1,\cdots,l;k_1,\cdots,k_\nu,\lambda=1,2).$$

Denote by $\mathfrak{R}'_l$ the open set of $\mathfrak{R}_l$ formed by all points such that $x^1\neq 0$ and $x^2\neq 0$. It is easy to see that $'\mathfrak{J}^0\mathfrak{R}_l\Sigma\cap\mathfrak{R}_l'$ is the submanifold of $\mathfrak{R}_l'$ defined by the conditions:

$$u^1{}_{2\,k_1\cdots k_{l-1}}=\epsilon(1,2,k_1,\cdots,k_{l-1})\cdot u^1\cdot(x_2x_{k_1}\cdots k_{l-1})^{-1};$$
$$u^2{}_{1\,k_1\cdots k_{l-1}}=\epsilon(1,2,k_1,\cdots,k_{l-1})\cdot u^2\cdot(x_1x_{k_1}\cdots k_{l-1})^{-1};$$
$$x_1u^1=x_2u^2=u.$$

Thus the dimension of the submanifold $'\mathfrak{J}^0\mathfrak{R}_l\Sigma\cap\mathfrak{R}_l'$ is 5 and the system of functions $x_1,x_2,u^1{}_{a_1\cdots a_l},u^2{}_{b_1\cdots b_l}$, where $a_1=\cdots=a_l=1$ and $b_1=\cdots=b_l=1$, and u can be considered as a system of coordinates on $'\mathfrak{J}^0\mathfrak{R}_l\Sigma\cap\mathfrak{R}_l'$. It is not hard to see that

$$d\Theta_{(1)12;k_1\cdots k_\nu},\quad d\Theta_{(2)12;k_1\cdots k_\nu},\quad d\Theta_{(3)12;a_1\cdots a_{\nu'}},\text{ and }d\Theta_{(3)12;b_1\cdots b_{\nu'}}$$
$$(\nu,\nu'=0,1,\cdots,l-1;a_1=\cdots=a_{\nu'}=1;$$
$$b_1=\cdots=b_{\nu'}=2;2\geqq k_1\geqq\cdots\geqq k_\nu),$$

are linearly independent modulo Ω at each point of $\mathfrak{R}_l'$. Their number is equal to $\dim\mathfrak{R}_l-5$. Therefore any point in $'\mathfrak{J}^0\mathfrak{R}_l\Sigma\cap\mathfrak{R}_{l'}$ is an ordinary integral point and satisfies (74). If y is in $'\mathfrak{J}^0\mathfrak{R}_l\Sigma\cap\mathfrak{R}_l'$ and if $a_1=\cdots=a_l=1$,

$$x_1d\Theta_{(1)12;a_1\cdots a_{l-1}}-x_2d\Theta_{(2)12;a_1\cdots a_{l-1}}-x_1x_2d\Theta_{(3)12;a_1\cdots a_{l-1}}$$
$$\equiv(x_1u^1{}_{a_1\cdots a_l}(y)+(l+1)!\,u(y)\cdot(x_1)^{-l})\omega^1$$

at y modulo ω^2 and Π_l. Since $u^1{}_{a_1\cdots a_l},x_1$, and u are independent variables on $'\mathfrak{J}^0\mathfrak{R}_l\Sigma\cap\mathfrak{R}_l'$, it follows that y is not a normal point of $(\mathfrak{R}_l\Sigma,\Omega)$.

INSTITUTE FOR ADVANCED STUDY AND NAGOYA UNIVERSITY.

REFERENCES.

[1] S. Bochner, *Lectures on commutative algebra*, 1938.

[2] E. Cartan, *Les systèmes différentiels extérieurs et leur applications géométriques*, Paris, 1945.

[3] ———, "Sur l'intégration des systèmes d'équations aux différentielles totales," *Annales Scientifiques de l'Ecole Normale Supérieure*, vol. 18 (1901), pp. 241-311.

[4] C. Chevalley, *Theory of Lie groups*, Princeton University Press, 1940.

[5] E. Kähler, "Einführung in die Theorie der Systeme von Differentialgleichungen," *Hamburger Mathematische Einzelschriften*, vol. 16 (1934).

[6] Y. Matsushima, "On a theorem concerning the prolongation of a differential system," *Nagoya Mathematical Journal*, vol. 6 (1953), pp. 1-16.

[7] P. Auslander, "An ideal theory for exterior differential systems," *Annals of Mathematics*, vol. 63 (1956), pp. 527-536.

[8] J. A. Schouten and W. v. d. Kulk, *Pfaff's Problem and its generalization*, Oxford, 1949.

UNIFORM SPACES WITH UNIQUE STRUCTURE.*

By W. F. Newns.

1. It has been proved by A. Weil [10] that a compact space has a unique uniform structure, and by Dieudonné [3] that a completely regular (or even completely normal [4]) space can have a unique structure without being compact. The problem of characterizing spaces with unique structure has been taken up by R. Doss [7], who has given a topological condition for the structure to be unique. It transpired also that a space with a unique structure is necessarily locally compact and that its Alexandroff compactification was the only possible compactification (cf. also [2]). It does not, however, seem to have been pointed out that this last property is *equivalent* to that of having a unique structure, a fact which is not quite obvious since there may conceivably be many structures on a space, but only one in which it is totally bounded.

Theorem 1. *In a completely regular space E, the following properties are equivalent:*

a) *E has a unique uniform structure;*

b) *E has a unique totally bounded uniform structure;*

c) *Of any pair of normally separable closed subsets of E, one at least is compact;*

d) *Each vicinity for each uniform structure on E contains a set of the form $A \times A$, where A is the complement of a compact subset of E.*

Any space having these properties is locally compact, and if not compact its unique compactification is its Alexandroff compactification.

The property c) is the one given by Doss: two closed subsets A and B are said to be normally separable if there exists a continuous mapping f of E into the compact interval $[0,1]$ such that $f(x) = 0$ for $x \in A$ and $f(x) = 1$ for $x \in B$.

If E is compact, the properties are evident, so that we assume henceforth that E is not compact. In this case, the complements of relatively

* Received August 16, 1956.

compact subsets of E form a filter, and the property d) is clearly equivalent to:

d′) The filter $\mathfrak{F}$ of complements of relatively compact subsets is a Cauchy Filter for every uniform structure on E.

That d′) implies a) has been proved by Dieudonné [3, 291] by observing that any ultrafilter on E must either converge or be finer than $\mathfrak{F}$, and hence that any completion of E has just one extra point and is compact, i.e., is the Alexandroff compactification. The property d) is useful in establishing that a given space has a unique structure (cf. [3], and [1, Chap. II, § 4, Exerc. 12]).

It is obvious that a) implies b). To show that b) implies c), let $\mathcal{U}_0$ be the unique totally bounded structure. Since any structure $\mathcal{U}$ on E is finer than some totally bounded structure [1, Chap. IX, § 1, Exerc. 6], it is finer than $\mathcal{U}_0$. Thus $\mathcal{U}_0$ is the coarsest structure on E and is therefore the Alexandroff structure [*ibid.*, Exerc. 11]: the completion $\hat{E}$ has just one point ω at infinity. Now let A and B be closed subsets of E normally separated by f. Since $\hat{E}$ is the Stone-Čech compactification of E, f is uniformly continuous in the structure induced on E by that of $\hat{E}$, and hence extends to $\hat{E}$. If A is not compact, we have $\omega \in \bar{A}$, so that $f(\omega) = 0$. Thus $\omega \notin \bar{B}$ (otherwise $f(\omega) = 1$) so that B is closed in $\hat{E}$ and therefore compact.

Since the last part of the theorem has already transpired, it remains only to prove that c) implies d′): i.e., that given any continuous écart f and any $\epsilon > 0$, there exists $A \in \mathfrak{F}$ such that $f(x, y) \leqq \epsilon$ whenever $x \in A$ and $y \in A$. Let $V = f^{-1}([0, \epsilon/3])$ and suppose that $V(z)$ is not compact: then since $V(z)$ and the set $\{y : f(y, z) \geqq \epsilon/2\}$ can be normally separated, the latter must be compact, and hence its complement A must belong to $\mathfrak{F}$. If x and y are any two points of A we have $f(x, y) \leqq f(x, z) + f(y, z) \leqq \epsilon$ as required. It remains to prove the existence of z. Now if no such z existed, then $V(x)$ would be compact for all $x \in E$, so that E would be complete and paracompact [1, Chap. II, § 4, Exerc. 10], hence normal [6]. But this means that, contrary to hypothesis, E would be compact in view of the following:

A normal space satisfying c) *is countably compact.*

For if not, there would exist in E a sequence (x_n) of distinct points without a limit point. The sets $\{x_{2n}\}$ and $\{x_{2n+1}\}$ would then be closed and disjoint hence normally separable, contrary to c) since neither is compact.

This completes the proof of Theorem 1, so that the result just proved may be stated:

THEOREM 2. *A normal space with a unique structure is countably compact.*

This is, in fact, a special case of a known result [1, Chap. IX, § 4, Exerc. 24] to the effect that a normal space which is totally bounded in all its structures is countably compact. Contrary to a statement by Dickinson [2, Theorem 3], the assumption that the space is normal cannot be omitted from the result. Miss Dickinson showed that the sets $\{x_{2n}\}$ and $\{x_{2n+1}\}$ could be enclosed in disjoint neighbourhoods (without assuming normality) and then asserted that the condition c) is violated (thus implicitly assuming normality). We shall now exhibit a space with a unique structure which is not countably compact.

Let ω, Ω be respectively the first ordinals of the second and third kind, E_0, F_0 the intervals $[1, \omega]$, $[1, \Omega]$ endowed with the open interval topology, and T the complement in $E_0 \times F_0$ of the point (ω, Ω). The space T was first discussed by Tychonoff [8] and has been shown to have a unique structure by Dieudonné [3]. It is clear that T is not countably compact (contrary to [5, § 4]), the sequence $\{(n, \Omega)\}$, for instance, having no limit point. It is easy, moreover, to verify directly that the sets $A = \{(2n, \Omega)\}$ and $B = \{(2n-1, \Omega)\}$ have disjoint neighbourhoods but are not normally separable. Indeed, if V is any neighbourhood of Ω in F_0, the sets $\{n\} \times V$ are mutually disjoint, and suitable unions form the required disjoint neighbourhoods: if f separated A and B, then for each n we could find α_n such that for $x \geqq \alpha_n$ we have $f(n, x) \leqq \frac{1}{4}$ or $f(n, x) \geqq \frac{3}{4}$ according as n is odd or even; if $\alpha < \Omega$ majorised $\{\alpha_n\}$, we should then have $f(n, \alpha) \leqq \frac{1}{4}$ for n odd and $f(n, \alpha) \geqq \frac{3}{4}$ for n even, contrary to the continuity of f at the point (ω, α).

2. It is natural to ask whether the property of having a unique structure is inherited by subspaces. Since frontier points are potential points at infinity, it is the closed subspaces which are most likely to have this property.

THEOREM 3. *A closed subspace of a normal space with a unique structure has itself a unique structure.*

For let A, B be normally separable closed subsets of the closed subspace F of E. Then A and B are closed in E and disjoint, hence normally separable. Since E has a unique structure, either A or B is compact, so that F satisfies the condition c) of Theorem 1 and hence has a unique structure.

A glance at Tychonoff space above will show that the result may fail in non-normal spaces. Indeed, the assumption that E is normal is *necessary*.

THEOREM 4. *If every closed subspace of a completely regular space E has a unique structure, then E is normal.*

For let A be any closed subset of E and f a continuous real-valued function defined on A. The closure $\tilde{A}$ of A in the completion $\tilde{E}$ of E is the completion of A for its unique structure. The function f, being uniformly continuous on A, extends by continuity to $\tilde{A}$; but since $\tilde{E}$ is normal, f may be further extended to $\tilde{E}$, and its restriction to E is then a continuous extension of f from A to E.

A subspace may have a unique structure without being closed, as is shown by regarding a non-compact space with unique structure as a subspace of its compactification. However, it is clear that a subspace with unique structure must either be closed or have a compact closure. In particular, this means that the closure of a subspace with unique structure also has unique structure.

The union of two sets with unique structure need not have a unique structure: the topological sum of two spaces with unique structure (and non-compact) will have two distinct structures, the Stone-Čech compactification providing two points at infinity.

The intersection of two sets with unique structure need not have a unique structure: in the compact space $E_0 \times F_0$ above, the subspace $E_0 \times \{\Omega\}$ is compact, but its intersection with T has not a unique structure.

3. The product of two spaces with unique structure will not in general have a unique structure. Indeed, if a product has a unique structure, then either one of the factors is trivial (i.e., consists of a single point) or both are compact: for let E be non-compact, F non-trivial, E_0, F_0 compactifications of E and F respectively, ω a point at infinity in E_0 and x, y distinct points of F; then $E_0 \times F_0$ is a compactification of $E \times F$ having two distinct points at infinity, namely (ω, x) and (ω, y).

If E is a space with unique structure and R an equivalence relation on E such that E/R is completely regular, then the quotient space will also have a unique structure. This is an immediate corollary of the following result:

THEOREM 5. *Let E be a space with unique structure and f a continuous mapping of E into a completely regular space. Then $f(E)$ has a unique structure.*

For if A, B are closed in $f(E)$ and normally separated by a function g, $f^{-1}(A)$ and $f^{-1}(B)$ are closed in E and normally separated by the function

$g \circ f$. By Theorem 1, one of these sets, say $f^{-1}(A)$, is compact, and hence so is $A = f(f^{-1}(A))$. Applying Theorem 1 again, we see that $f(E)$ has a unique structure.

4. Let E be a space with unique structure, F a completely regular space and f a continuous $(1,1)$ mapping of E onto F. Then if E is compact, so is F, and f is a homeomorphism. *The mapping f will also be a homeomorphism in the case where F* (and hence E) *is non-compact:* for if F_0 is any compactification of F, f is uniformly continuous as a mapping of E into F_0, hence extends to a mapping $\bar{f}$ of $\tilde{E}$ onto F_0, onto since $\bar{f}(\tilde{E})$ is compact and everywhere dense; since $\tilde{E}$ has just one point at infinity, so has F_0, and $\bar{f}$ is $(1,1)$, hence a homeomorphism.

The case where F is compact but E is not can easily be seen to occur, so that f will not always be a homeomorphism. We need only take E to be a non-compact space with unique structure and F the quotient space obtained by identifying, in $\tilde{E}$, some point of E with the point at infinity. It follows that the topology of a (non-compact) space with unique structure is not a minimal completely regular topology, though all strictly coarser topologies must be compact (cf. [9]).

UNIVERSITY OF LIVERPOOL.

REFERENCES.

[1] N. Bourbaki, *Topologie Generale*, 1940-1949. Paris, Hermann.

[2] A. Dickinson, "Compactness conditions and uniform structure," *American Journal of Mathematics*, vol. 75 (1953), pp. 224-228.

[3] J. Dieudonné, "Sur les espaces uniformes complets," *Annales Scientifiques de l'Ecole Normale Superieure*, vol. 56 (1939), pp. 277-291.

[4] ———, "Un exemple d'espace normal non susceptible d'une structure uniforme d'espace complet," *Comptes Rendus*, vol. 209 (1939), pp. 145-147.

[5] ———, "Sur les espaces topologiques susceptibles d'être munis d'une structure uniforme d'espace complet," *ibid.*, vol. 209 (1939), pp. 666-668.

[6] ———, "Une généralisation des espaces compacts," *Journal de Mathématiques Pures et Appliquées*, New Series, vol. 23 (1944), pp. 65-76.

[7] R. Doss, "On uniform spaces with unique structure," *American Journal of Mathematics*, vol. 71 (1949), pp. 19-23.

[8] A. Tychonoff, "Über die topologische Erweiterung von Raümen," *Mathematische Annalen*, vol. 102 (1930), pp. 544-561.

[9] Jungo Wada, "Lattices of spaces," *Osaka Mathematical Journal*, vol. 5 (1953), pp. 1-5.

[10] A. Weil, *Sur les espaces à structure uniforme*, 1937. Paris, Hermann.

THE CRITERIA FOR ALGEBRAIC EQUIVALENCE AND THE TORSION GROUP.*[1]

By T. Matsusaka.

Let V be a variety in a projective space, non-singular in co-dimension 1. We assume that the reader is familiar with the notion of numerical, algebraic and linear equivalence of divisors, as well as algebraic families of divisors (Weil [14], Chow-v. d. Waerden [2]). Let us denote by $G(V)$, $G_a(V)$ and $G_l(V)$ the groups of V-divisors, V-divisors algebraically equivalent to 0 and V-divisors linearly equivalent to 0 respectively. When V is non-singular, let us denote by $G_n(V)$ the group of V-divisors numerically equivalent to 0. The set of V-divisors X, such that mX is in $G_a(V)$ for a certain positive integer m, forms a group containing $G_a(V)$ and the factor group of it with respect to $G_a(V)$ is called the *torsion group* of V-divisors. By Néron's result (Néron [8]) $G(V)/G_a(V)$ is finitely generated; therefore the torsion group of V-divisors is a finite group. One of the aims of this paper is to show that when V is non-singular, the torsion group is nothing but $G_n(V)/G_a(V)$. We shall prove this directly and we shall not assume Néron's result. Since we need an equivalence criterium for algebraic equivalence, first we shall settle that. This includes, as a special case, the criterium which is formulated in terms of the Poincaré normal function in the classical case of algebraic surfaces (Zariski [16], pp. 128-132).

Let V and V' be two complete non-singular varieties, and f be a birational transformation of V onto V'. Then it is not difficult to see that when Z is a V-divisor such that mZ is algebraically equivalent to 0 on V, $f^{-1}\cdot f(Z)=Z$. The same is true for V'-divisors of the same nature. From this it follows that the torsion group is an absolute invariant of a class of birationally equivalent non-singular complete varieties. But it is not so, when we consider a class of birationally equivalent complete varieties, non-singular in co-dimension 1. For instance, the quotient variety of an Abelian variety A by the group of automorphisms consisting of δ and $-\delta$, which is usually called the *ordinary Kummer variety* of A, is non-singular in co-dimension 1 and has a finite number of singular points; moreover, it is easy to see that it has

* Received March 15, 1956; revised October 17, 1956.

[1] This research was supported by the National Science Foundation.

a non-trivial torsion group of divisors. On the other hand, when we desingularize it, we get a complete non-singular variety without a torsion group of divisors, as was shown recently by Spanier (cf. E. Spanier, "The homology of Kummer Manifolds," *Proceedings of the American Mathematical Society*, vol. 7, 1956).

We assume that the reader is familiar with Weil's fundamental works (Weil [12], [13]) and we shall follow the same terminology and conventions. If two divisors X and Y on V are such that $X \equiv Y \bmod G_l(V)$, we shall write $X \sim Y$. We shall denote by $\mathfrak{A}^*$, $\mathfrak{L}^*$ cosets of $G(V)$ modulo $G_a(V)$ and $G_l(V)$ respectively. If $\mathfrak{A}^*$ or $\mathfrak{L}^*$ contains a divisor X, we shall write sometimes $\mathfrak{A}^*(X)$ or $\mathfrak{L}^*(X)$ for $\mathfrak{A}^*$ or $\mathfrak{L}^*$. In the same way, when V is non-singular, we shall denote by $\mathfrak{N}^*$ a coset of $G(V)$ modulo $G_n(V)$ and when it contains a divisor X, we shall write $\mathfrak{N}^*(X)$ for $\mathfrak{N}^*$. We shall denote by $\mathfrak{N}, \mathfrak{A}, \mathfrak{L}$ (resp. $\mathfrak{N}(X), \mathfrak{A}(X), \mathfrak{L}(X)$) the sets of positive divisors in $\mathfrak{N}^*, \mathfrak{A}^*, \mathfrak{L}^*$ (resp. $\mathfrak{N}^*(X), \mathfrak{A}^*(X), \mathfrak{L}^*(X)$). It is well-known that $\mathfrak{L}$ is an algebraic family, usually known as a *complete linear system*. Let X be a V-divisor and $L(X)$ be the module of rational functions f on V such that $(f) \succ -X$. We shall denote by $l(X)$ the dimension of $L(X)$ over the universal domain, which is $\dim \mathfrak{L}(X) + 1$, where $\dim \mathfrak{L}(X)$ means the dimension of $\mathfrak{L}(X)$ as an algebraic family, i.e. the smallest dimension of varieties which parametrize $\mathfrak{L}(X)$.

Let Y be a positive cycle in a projective space. Regarding the set of coefficients of the Chow-form (Zugeordnete Form) of Y, arranged in a certain order, as a set of homogeneous coordinates of a point, we call it the *Chow-point* of Y. If an integer d is given, the set of all positive V-divisors of degree d forms a finite set of algebraic families (Chow-v. d. Waerden [2]). Each such family is called a *maximal algebraic family* since it is not contained in another family consisting of positive divisors of the same degree. An algebraic family $\mathfrak{F}$ is called *total*, if for any V-divisor Z algebraically equivalent to 0, there is a divisor X in $\mathfrak{F}$ such that $Z \sim X - X_0$, for a fixed divisor X_0 in $\mathfrak{F}$ (Matsusaka [3], Th. 1). We shall say that an algebraic family is defined over a field K, if its Chow-variety (i.e. the set of corresponding Chow-points) is defined over K. About maximal algebraic families, we know the following results.

THEOREM 1. *Let V be a projective variety, non-singular in co-dimension 1, and C be a hyperplane section of V.* (i) *For a given divisor X, there is a positive integer m_0 such that whenever $m \geqq m_0$, there is a total maximal family in $\mathfrak{A}(X + mC)$.* (ii) *If $\mathfrak{F}$ and $\mathfrak{F}'$ are two total maximal families of*

divisors on V in the same coset $\mathfrak{A}^*$, then $\mathfrak{F}=\mathfrak{F}'$. (iii) *Assume that V is non-singular. If a V-divisor X is given, there is a positive integer m_0 having the following properties: whenever $m \geqq m_0$, $\mathfrak{A}(X+mC)$ itself is a total algebraic family; any two divisors in $\mathfrak{A}(X+mC)$ determine complete linear systems of the same dimension; and for any divisor Y in $\mathfrak{A}(X+mC)$, $\mathfrak{L}(Y)$ contains a non-singular variety.*

For these, see Matsusaka [5], Th. 2, Lemma 2.

We can define *specializations of cycles* on projective varieties. Specializations are compatible with the operations of addition, multiplication and algebraic projection. As far as positive cycles are concerned, specializations are compatible with the operation of intersection-product. Moreover, when the ambient variety is non-singular in co-dimension 1, algebraic equivalence and linear equivalence of divisors are preserved by specializations. For the general treatment of specializations, we refer to Shimura [10]. We shall write $X \to X'$ ref k, when a cycle X' is a specialization of a cycle X with reference to k.

Let V be a variety defined over a field k in a projective space and $H_1,\cdots,H_s$ be s independent generic hypersurfaces in the ambient space over k. Then $V\cdot H_1\cdots H_s$ is defined and is a variety; and it is non-singular (resp. non-singular in co-dimension 1) when V is non-singular (resp. non-singular in co-dimension 1) (Weil [14]). Let us call it a *general variety on V generic over k*. When we say that a variety W is a general variety on V, it is understood that W is a general variety on V, generic over a certain field of definition for V.

1. Let us fix once for all a projective variety V, non-singular in co-dimension 1 and an *algebraically closed* field of defintion k of V. We regard k as a basic field and all fields will be assumed to contain k.

LEMMA 1. *Let W be a general variety on V generic over k and K be a common field of definition for V and W. Let X and X' be V-divisors such that $X \to X'$ ref K and that $X\cdot W$ is defined. When*

(1) $(X, X\cdot W) \to (X', Y)$ ref K, (2) $(X, X\cdot W) \to (X', Y^*)$ ref K,

are two specializations of $(X, X\cdot W)$ over $X \to X'$ ref K, then Y and Y^* are linearly equivalent on W.[2]

Proof. First let us consider the case when X is positive . Then X' is

[2] The writer wishes to take this opportunity to correct the error in the proof of Prop. 2, Matsusaka [3]. Prop. 2 itself is an immediate consequence of this lemma.

also positive. We can find projecting cones R and R' of X and X' respectively such that

$$R\cdot V = X + N,\ R'\cdot V = X' + N',\ \deg(R) = \deg(R') = \deg(X) = \deg(X'),$$

that $N\cdot W$, $N'\cdot W$ are both defined and that R' is the uniquely determined specialization of R over the specialization $X\to X' \operatorname{ref} K$ (for projecting cones, see v. d. Waerden [11], pp. 634-635). Let H be a hypersurface of the same degree as R defined over K such that $H\cdot V$ and $H\cdot W$ are both defined. We have $X\sim H\cdot V - N$, $X'\sim H\cdot V - N'$. By the compatibility of specializations with the operation of intersection-product, $X\to X' \operatorname{ref} K$ determines uniquely the specialization $(X, N, N\cdot W)\to (X', N', N'\cdot W) \operatorname{ref} K$. Hence (1) and (2) determine uniquely specializations

$$(1')\qquad (X, X\cdot W, N, N\cdot W)\to (X', Y, N', N'\cdot W) \operatorname{ref} K,$$

$$(2')\qquad (X, X\cdot W, N, N\cdot W)\to (X', Y^*, N', N'\cdot W) \operatorname{ref} K.$$

Since linear equivalence is preserved by specializations and since $X\cdot W \sim H\cdot W - N\cdot W$, we get, from (1') and (2'), the following relations: $X\sim H\cdot W - N'\cdot W$, $Y^*\sim N\cdot W - N'\cdot W$. This proves our lemma in the case when X is positive.

Suppose that X is not positive and write $X = X_1 - X_2$, $X_i \succ 0$ for $i = 1, 2$. Let

$$(X, X\cdot W, X_1, X_2, X_1\cdot W, X_2\cdot W)\to (X', Y, X_1', X_2', Z_1, Z_2) \operatorname{ref} K,$$

$$(X, X\cdot W, X_1, X_2, X_1\cdot W, X_2\cdot W)\to (X', Y^*, X_1', X_2', Z_1^*, Z_2^*) \operatorname{ref} K,$$

be extensions of (1) and (2) respectively. We have $X' = X_1' - X_2'$ and by what we have seen already in the case of positive divisors, $Z_1\sim Z_2^*$, $Z_2\sim Z_2^*$. Since $X\cdot W = X_1\cdot W - X_2\cdot W$, we have $Y = Z_1 - Z_2$ and $Y^* = Z_1^* - Z_2^*$, which prove that $Y\sim Y^*$. Thus our lemma is proved.

LEMMA 2. *Let U be a variety in a projective space L_1 and f be a rational mapping of U into a projective space L_2 such that f is everywhere single-valued. Let X be a subvariety of U and X' be a specialization of X over a common field of definition K for U and f. If the image of X by f is a d-dimensional variety, there is a component of X' such that its image by f has at least dimension d.*

Proof. It is clear that if our lemma is true when U is a normal variety, it is true in general, by passing from the given variety to its derived normal variety. Therefore, let us assume that U is a normal variety. Let Z be the

graph of f. By our assumption, f is everywhere defined on U. There is a uniquely determined subvariety X^* of Z of the same dimension as X with the projection X on U (Weil [12], Chap. 4, Th. 15). Let $(X, X^*) \to (X', Y)$ ref K be an extension of $X \to X'$ ref K on $L_1 \times L_2$. By the compatibility of specializations with the operation of algebraic projection, we see that $\mathrm{pr}_1 Y = X'$, where pr_1 is the operation of algebraic projection on the first factor of the product $L_1 \times L_2$. Hence if $X' = \sum a_i Z_i$ is the reduced expression for X', $Y = \sum a_i Z_i^*$ is the reduced expression for Y, where Z_i^* is the uniquely determined subvariety of Z with the projection Z_i on U.

Let H be a generic linear variety of co-dimension d in L_2 over a field over which X, X' are both rational and $K(u)$ be the smallest field of definition for H containing K. Then $(X, X^*) \to (X', Y)$ ref $K(u)$ on $L_1 \times L_2$. Since $X^* \cdot (L_1 \times H)$, $Y \cdot (L_1 \times H)$ are both defined (Weil [12], Chap. 5, Prop. 2), we see that $X^* \cdot (L_1 \times H) \to Y \cdot (L_1 \times H)$ ref $K(u)$ on $L_1 \times L_2$. Because of the fact that the former is not empty, the latter cannot be empty. This proves our lemma.

LEMMA 3. *Assume that V is normal and let X be a positive V-divisor. Let K be a field of definition for V over which X is rational and let C be a hyperplane section of V, generic over K. There is a positive integer h_0 such that whenever $h \geqq h_0$, the complete linear system $\mathfrak{L}(X + hC)$ induces a complete linear system on C.*

This is the so-called Castelnuovo lemma in the classical case. As to the proof, see Matsusaka [5], p. 126.

2. Let us recall some of the known results on Picard varieties which we shall need later. Let U be a complete algebraic variety, non-singular in co-dimension 1 and K be a field of definition for U. Let G be a subset of $G(U)$ and f be a mapping of G into an algebraic variety W with the following properties: (i) f is defined outside of a proper subset of G; (ii) there is a common field of definition K' for U and W such that when Z is a divisor in G, rational over a field K^* containing K', $f(Z)$ is rational over K^* if it is defined. When f satisfies the above conditions, then we shall say that f is a *rational mapping* of G and K' is a *field of definition* of f. Moreover, if G is a subgroup of $G(U)$, W a group variety and f a group-homomorphism, we shall say that f is a *rational homomorphism.* There is an Abelian variety P and a rational homomorphism f of $G_a(U)$ onto P such that the kernel of f is $G_l(U)$ and that f has the universal mapping property as a rational homomorphism of $G_a(U)$ into an Abelian variety. P is called the

Picard variety of U and f is called the *canonical homomorphism* of $G_a(U)$ onto P. When U is a projective variety, we may take P, f to be defined over K and when $\dim U > 2$, the Picard variety of U and the Picard variety of a general variety on U of dimension at least 2 differ by a purely inseparable homomorphism. As to these, see Chow [1]; Matsusaka [3], [4], [6], [7]; Néron-Samuel [9].

Let us asume, from now on, that V is a *normal variety*. Let W be a general variety on V generic over k and $k(u)$ be the smallest field of definition for W. Then $k(u)$ is a purely transcendental extension of k. We regard (u) as a parameter on which W depends over the field k, and we shall write sometimes W_u for W. W is a normal variety since V is normal (Zariski [15], Th. 3). Let us denote by $P(V)$ and $P(W)$ the Picard varieties of V and W. Then as we have remarked already, we may assume that $P(V)$, $P(W)$ are defined over k and over $k(u)$ respectively, together with the canonical homomorphisms. Let $\mathfrak{F}$ be an algebraic family of positive V-divisors defined over a field K and assume that W_u is a general variety on V generic over K. Let X be a generic divisor of $\mathfrak{F}$ over $K(u)$; then $X \cdot W_u$ is defined and is rational over a regular extension of $K(u)$. Let $\mathfrak{F}'$ be the set of specializations of $X \cdot W_u$ over $K(u)$, which we shall call the *family induced on W_u by $\mathfrak{F}$*.

LEMMA 4. *Let $\mathfrak{F}$ and $\mathfrak{F}^*$ be two total maximal families of positive V-divisors and W_u be a general variety generic over a common field K of definition for $V, \mathfrak{F}$ and $\mathfrak{F}^*$. Let X and X^* be generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ over $K(u)$ and assume that $\mathfrak{L}(X)$, $\mathfrak{L}(X^*)$ induce again on W_u complete linear systems.* (i) *If $\dim W_u = 1$ and if the induced families $\mathfrak{F}'$, $\mathfrak{F}^{*\prime}$ contain W_u-divisors linearly equivalent to each other on W_u, then $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ coincide.* (ii) *If $\dim W_u > 1$ and if $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ contain divisors algebraically equivalent to each other on W_u, then $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ coincide.*

Proof. According to Weil's equivalence criteria for linear equivalence (Weil [14], Cor. 2, Th. 7), any V-divisor Z such that $Z \cdot W_u \sim 0$ on W_u is linearly equivalent to 0 on V, provided Z is algebraically equivalent to 0. Let us omit to write u and let $P(W)$ and f be the Picard variety of W and the canonical homomorphism of $G_a(W)$ onto $P(W)$, both defined over $K(u)$. Let us assume that $\dim W = 1$; let Y and Y^* be W-divisors contained in $\mathfrak{F}', \mathfrak{F}^{*\prime}$ which are linearly equivalent to each other on W and T, T^* be the loci of $f(X \cdot W - Y)$, $f(X^* \cdot W - Y^*)$ over the algebraic closure of $K(u)$ respectively. Then T and T^* are Abelian varieties in $P(W)$ and $T = T^*$ since $\mathfrak{F}$ and $\mathfrak{F}^*$ are maximal total families. T is isogenous to the Picard variety $P(V)$ of V (in fact, differs from $P(V)$ by a purely inseparable homo-

morphism) by Weil's equivalence criteria for linear equivalence. Let x be a generic point of T over the algebraic closure K' of $K(u)$. Then by the main theorem on Jacobian varieties (Weil [13], Th. 19), there is a positive W-divisors Z of the same degree as Y, Y^* such that $f(Z-Y)=x=f(Z-Y^*)$. Let X_1 and X_1^* be generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ over $K(u)$ such that $f(X_1\cdot W-Y)=x=f(X_1^*\cdot W-Y^*)$. Then $X_1\cdot W\sim X_1^*\cdot W\sim Z$. By our assumption, $\mathfrak{L}(X_1), \mathfrak{L}(X_1^*)$ induce on W complete linear systems. Therefore, $\mathfrak{L}(X_1)=\mathfrak{L}(X_1^*)=\mathfrak{L}(Z)$ and $\mathfrak{L}(Z)$ is contained in both $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$. Let K^* be a field of definition for the algebraic family $\mathfrak{L}(Z)$ containing K' and Z^* be a generic divisor of $\mathfrak{L}(Z)$ over K^*. Then $X_1\cdot W$ and $X_1^*\cdot W$ are specializations of Z^* over K^* and, a fortiori, over K'. This proves (i) when we take the definition of induced families into account.

Assume that $\dim W>1$. The same equivalence criteria of Weil show that $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ are total families on W since $P(V)$ and $P(W)$ have the same dimension in this case (Chow [1], Matsusaka [7]). By our assumption, $\mathfrak{F}', \mathfrak{F}^{*\prime}$ contain divisors Y and Y^* which are algebraically equivalent to each other on W. Hence $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ coincide by Th. 1, (ii), provided both are maximal families. But since generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ over $K(u)$ are such that the complete linear systems determined by them induce on W complete linear systems by our asumption, $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ must be maximal. Our lemma is thereby proved.

PROPOSITION 1. *Let $\mathfrak{F}$ and $\mathfrak{F}^*$ be two total families on V; let K be an algebraically closed common field of definition for V, $\mathfrak{F}$ and $\mathfrak{F}^*$; let W_u be a general variety on V generic over K and $\mathfrak{F}'$, $\mathfrak{F}^{*\prime}$ be the families induced on W_u by $\mathfrak{F}$ and $\mathfrak{F}^*$ respectively. Assume that $\mathfrak{F}'=\mathfrak{F}^{*\prime}$.* (i) *When* $\dim W_u=1$, *there is a finite set of subvarieties $D_1,\cdots,D_s$ of V depending only upon W_u such that if X and X^* are divisors in $\mathfrak{F}$ and $\mathfrak{F}^*$ respectively, $X-X^*$ is algebraically equivalent to a linear combination $\sum m_iD_i$ of the D_i. The D_i have the property that $\sum a_iD_i\equiv 0 \bmod G_a(V)$ if and only if $a_i=0$.* (ii) *When* $\dim W_u>1$, *$\mathfrak{F}$ and $\mathfrak{F}^*$ belong to the same coset of $G(V) \bmod G_a(V)$.*

When $\mathfrak{F}$ and $\mathfrak{F}^*$ are both maximal and total, then $\mathfrak{F}=\mathfrak{F}^*$ if every $m_i=0$ in the case when $\dim W_u=1$. *$\mathfrak{F}=\mathfrak{F}^*$ when* $\dim W_u>1$.

Proof. Let X and X^* be generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ respectively over $K(u)$ and C be a hyperplane section of V rational over K. By using our Lemma 3, we see that when m is sufficiently large, $\mathfrak{L}(X+mC)$ and $\mathfrak{L}(X^*+mC)$ again induce on W_u complete linear systems. Let $\mathfrak{F}_1$ and $\mathfrak{F}_1^*$ be maximal families containing $X+mC$ and X^*+mC respectively as members. Then it is easy to see that $\mathfrak{F}_1$ and $\mathfrak{F}_1^*$ are both maximal total families and by our assumption the induced families $\mathfrak{F}_1'$ and $\mathfrak{F}_1^{*\prime}$ contain

common W_u-divisors. By our choice of X, X^* and C, $X+mC$ and X^*+mC are linearly equivalent to generic divisors of $\mathfrak{F}_1$ and $\mathfrak{F}^*$ respectively over $K(u)$. Therefore, $\mathfrak{F}_1'$ and $\mathfrak{F}_1^{*\prime}$ coincide by Lemma 4. If (i) and (ii) are true for $\mathfrak{F}_1$ and $\mathfrak{F}_1^*$, they are also true for $\mathfrak{F}$ and $\mathfrak{F}^*$. Hence let us assume that $\mathfrak{F}$ and $\mathfrak{F}^*$ are both total and maximal.

Let U and U^* be the Chow-varieties of $\mathfrak{F}$ and $\mathfrak{F}^*$ (the set of Chow-points of divisors in $\mathfrak{F}$ and $\mathfrak{F}^*$) and x, x^* be the Chow-points of X, X^*. Let h_u, h_u^*, g_u be the rational mappings from U, U^* and from $U\times U^*$ defined as follows:

$$h_u(x)=f_u((X-X_0)\cdot W_u); \qquad h_u^*(x^*)=f_u((X^*-X_0)\cdot W_u);$$
$$g_u(x\times x^*)=f_u((X-X^*)\cdot W_u),$$

where X_0 is a fixed rational divisor in $\mathfrak{F}$ over K and f_u is the canonical homomorphism of $G_a(W_u)$ onto $P(W_u)$. Since W_u is defined over $K(u)$, we may assume that $P(W_u)$ and f_u are both defined over $K(u)$. Of course, the second and third formulas have a meaning by our assumption; $h_u(x)$ and $h_u^*(x^*)$ have the same locus A_u over $K(u)$, which is an Abelian variety on $P(W_u)$ and differs from the Picard variety $P(V)$ of V by a purely inseparable homomorphism. Let us observe that h_u, h_u^* and g_u are everywhere single-valued rational mappings defined over $K(u)$; this is an immediate consequence of our Lemma 1.

Let 0_u be the neutral element of $P(W_u)$ as a group, which is also the same for the group A_u. Let us prove that $g_u^{-1}(0_u)$ contains a component Z_u defined over a purely inseparable extension of $K(u)$ such that when $y\times y^*$ is a generic point of Z_u over the algebraic closure of $K(u)$, y and y^* are generic points of U and U^* over $K(u)$. We have $g_u(x\times x^*)=h_u(x)-h_u^*(x^*)$ and hence $g_u^{-1}(0_u)$ consists of points $y'\times y^{*\prime}$ such that $h_u(y')=h_u^*(y^{*\prime})$. Let us put $h_u(x)=w$. It is not difficult to see that $h_u^{-1}(w)$ consists of Chow-points of divisors contained in $\mathfrak{L}(X)$ by Weil [12], Chap. 6, Th. 11 and by the criteria for linear equivalence. Let y^* be a generic point of U^* over $K(u)$ such that $h_u^*(y^*)=w$ and Y^* be the divisor in $\mathfrak{F}^*$ with the Chow-point y^*. Then again $h_u^{*-1}(w)$ consists of Chow-points of divisors in $\mathfrak{L}(Y^*)$. Therefore, the point sets $|h_u^{-1}(w)|$, $|h_u^{*-1}(w)|$ are the point sets of Chow-varieties of $\mathfrak{L}(X), \mathfrak{L}(Y^*)$ respectively. Let us assume that x and y^* are independent generic points of $|h_u^{-1}(w)|$, $|h_u^{*-1}(w)|$ over the algebraic closure of $K(u,w)$; let Z_u be the locus of $x\times y^*$ over the algebraic closure of $K(u)$. We see that Z_u is contained in a component of $g_u^{-1}(0_u)$ and x, y^* are generic points of U, U^* over $K(u)$. Let T be a component of $g_u^{-1}(0_u)$ containing Z_u and $t\times t^*$ be a generic point of T over the algebraic closure

of $K(u)$. Then $h_u(t) = h_u^*(t^*) = w'$ is a generic point of A_u over $K(u)$ and is a generic specialization of w over the algebraic closure of $K(u)$. Therefore, by our choice of x, y^*, $t \times t^*$ must be a generic specialization of $x \times y^*$ over the algebraic closure of $K(u)$. This proves that $T = Z_u$. Now let $(Z_u', x', y^{*\prime})$ be a generic specialization of (Z_u, x, y^*) over $K(u)$. Then $h_u(x') = h_u^*(y^{*\prime}) = w'$ is a generic specialization of w over $K(u)$. Since A_u is defined over $K(u)$, it follows that w' is also a generic specialization of w over the algebraic closure of $K(u)$. Therefore $(w, h_u^{-1}(w), h_u^{*-1}(w))$ is a generic specialization of $(w', h_u^{-1}(w'), h_u^{*-1}(w'))$ over the algebraic closure of $K(u)$. This shows that Z_u and Z_u' coincide by the definition of Z_u. Thus our assertion is proved.

Now we are in position to prove our proposition. Let $\mathfrak{S}$ be the set of specializations of Z_u over K in the ambient space of $U \times U^*$; $\mathfrak{S}$ is an algebraic family of varieties defined over K and Z_u is a generic variety of it over K. Let u' be an independent generic specialization of u over K, then $Z_{u'}$ is also a generic variety of $\mathfrak{S}$ over K. Moreover, $Z_{u'}$ is also a generic variety of $\mathfrak{S}$ over $K(u)$ and consequently Z_u is a specialization of $Z_{u'}$ over $K(u)$. Since g_u is everywhere single-valued and since Z_u is such that every point on it is mapped to one and the same point 0_u, it follows that every point on $Z_{u'}$ is mapped also to one and the same point by g_u according to Lemma 2. Let us denote such a point on $P(W_u)$ by $Q(u')$. Since $Z_{u'}$ is defined over a purely inseparable extension of $K(u')$, there is a positive integer m such that it is defined over $K(u'^{p^{-m}})$, where $K(u'^{p^{-m}})$ is the image of $K(u')$ by the automorphism of the universal domain defined by $z \to z^{p^{-m}}$. Let R be the locus of $v' = u'^{p^{-m}}$ over K, which is a rational variety since $K(u')$ is a purely transcendental extension of K. Put $v = u^{p^{-m}}$. We get a rational mapping f from R into $P(W_u)$ defined over $K(u)$ such that $f(v') = Q(u')$ and that $(v, Q(u))$ is a specialization of $(v', Q(u'))$ over $K(u)$. On the other hand, every rational mapping from a rational variety into an Abelian variety is a constant by Weil [13], Cor., Th. 8. Hence $f(v') = Q(u') = 0_u$ and from this we see that $(X - Y^*) \cdot W_u \sim 0$ on W_u. Therefore, when $\dim W_u > 1$, $X \sim Y^*$ and when $\dim W_u = 1$, $X - Y^* \sim \sum m_i D_i$ where the D_i are subvarieties of V having the properties stated in our proposition (Weil [14], Cor., Prop. 5). Thus we have proved (i) and (ii). The rest of our assertion follows from Theorem 1.

Let C be a general curve on V generic over k, J be the Jacobian variety of C and ϕ be the canonical function of C into J. Let us associate to every positive V-divisor X the point

$$S(\phi(C \cdot X)) = f(X),$$

which is the sum of the components of $C \cdot X$ on J. In the case when $C \cdot X$ is not defined, let Y be a divisor linearly equivalent to X such that $C \cdot Y$ is defined, then we define $f(X) = f(Y)$. This definition is compatible with specializations by Lemma 1.

Let $\mathfrak{F}$ be a total family on V defined over k and X_0 be a fixed rational divisor in $\mathfrak{F}$ over k. When X is a generic divisor of $\mathfrak{F}$ over a common field of definition K for C, J and $\phi, f(X) - f(X_0)$ has a locus A over K which is an Abelian variety in J, and differs from the Picard variety of V by a purely inseparable homomorphism. Let us prove the following theorem.

THEOREM 2. *Let C, J, ϕ, A be as described and Y, Y' be two positive divisors of the same degree on V. Let $D_1, \cdots, D_s$ be subvarieties of V with the properties stated in Prop. 1. If Y and Y' are algebraically equivalent to each other, $f(Y)$ and $f(Y')$ differ by a point of A. Conversely, when $f(Y) - f(Y')$ is a point of A, $Y - Y'$ is algebraically equivalent to a linear combination of $D_1, \cdots, D_s$.*

Proof. Suppose that $Y - Y'$ is algebraically equivalent to 0. Let $\mathfrak{F}$ be a total family on V and X_0 be a fixed divisor in $\mathfrak{F}$. There is a divisor X in $\mathfrak{F}$ such that $Y - Y' \sim X - X_0$. Hence $f(Y) = f(Y') = f(X) - f(X_0)$ which is a point on A. Therefore, we get the first assertion.

Let W be a hyperplane section of V and let us take m so large that there are total maximal families $\mathfrak{G}, \mathfrak{G}'$ such that $\mathfrak{G}$ is contained in $\mathfrak{A}(Y + mW)$ and $\mathfrak{G}'$ is contained in $\mathfrak{A}(Y' + mW)$ (cf. Th. 1.). Let K be an algebraically closed common field of definition for $V, C, J, \phi, A, \mathfrak{F}, \mathfrak{G}, \mathfrak{G}'$ and Z and Z' be generic divisors of $\mathfrak{G}$ and $\mathfrak{G}'$ over K. By the Lemma 3, we may assume that $\mathfrak{L}(Z)$ and $\mathfrak{L}(Z')$ induce on C complete linear systems. Since $\mathfrak{G}$ and $\mathfrak{G}'$ are total, the loci of $f(Z), f(Z')$ over K are of the form $A_b, A_{b'}$. Our assumption shows that $f(Y + mW) = f(Y' + mW) + a$ where a is a point on A. Hence $A_b, A_{b'}$ have a point in common, and consequently $A_b = A_{b'}$. On the other hand, since $\mathfrak{L}(Z)$ and $\mathfrak{L}(Z')$ induce on C complete linear systems, $\mathfrak{G}$ and $\mathfrak{G}'$ induce on C the same algebraic family, as can be seen easily by using the fundamental theorem on Jacobian varieties (Weil [13], Th. 19). Then our assertion follows from Prop. 1.

Remark. It is very desirable to eliminate the subvarieties $D_1, \cdots, D_s$ from our theorem. In order to do so, we have to eliminate them from Weil's equivalence criteria. In particular, we have to do so for Weil [13], Th. 2. Suppose that W is a general surface on V generic over k. Assume that W has the property that the generic linear pencil contained in the linear system of hyperplane sections on W does not contain reducible members. Let H be

a generic hyperplane with respect to V and W and take $W \cdot H$ to be a general curve on V generic over k. Then we can eliminate those special subvarieties from the equivalence criteria for linear equivalence and our theorem becomes as follows.

The necessary and sufficient condition that Y and Y' are algebraically equivalent is that $f(Y)$ and $f(Y')$ differ by a point of A.

Those algebraic surfaces which do not fulfill the above mentioned property are known to be the *ruled surfaces* or the *Steiner surfaces* in the classical case. But this difficulty may be avoided by applying a birational transformation to V. In fact, there is a normal projective variety V', birationally equivalent to V, such that a general surface on V' has the above mentioned property (cf. Néron-Samuel [9], § 4).

THEOREM 3. *Let W be a general variety on V generic over k; let Z be a V-divisor such that $Z \cdot W$ is defined. When* $\dim W \geqq 2$ *and $Z \cdot W$ is algebraically equivalent to* 0 *on W, Z is algebraically equivalent to* 0 *on V.*

Proof. Let us write Z as the difference $X - X^*$ of two positive divisors. Since we are interested in algebraic equivalence, we may replace Z by another V-divisor algebraically equivalent to Z. In particular, we may assume that Z is rational over k since k is algebraically closed. Let C be a hyperplane section of V, rational over k and let $\mathfrak{F}$ and $\mathfrak{F}^*$ be total maximal families contained in $\mathfrak{A}(X+mC)$ and $\mathfrak{A}(X^*+mC)$ for sufficiently large m (cf. Th. 1). By Lemma 3, we may assume that the complete linear systems determined by generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ over a common field K of definition for V and W induce on W complete linear systems, by taking m sufficiently large. Our assumption shows that the induced families $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ on W by $\mathfrak{F}$ and $\mathfrak{F}^*$ contain divisors algebraically equivalent to each other on W. Therefore, by Lemma 4, (ii), $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ coincide and consequently $\mathfrak{F}$ and $\mathfrak{F}^*$ coincide by Prop. 1. This proves that Z is algebraically equivalent to 0.

3. Let us assume here that V is a *non-singular algebraic surface.*

PROPOSITION 2. *Let X and X' be V-divisors numerically equivalent to each other. Then the virtual arithmetic genus $p_a(X)$ of X and that of X' coincide* (for the definition of the virtual arithmetic genus, see Zariski [15]).

Proof. Let $K(V)$ be a canonical divisor of V. Let us assume first that X and X' are both non-singular curves. Since $\mathfrak{L}(X+K(V))$ induces on X a linear system contained in the canonical system (Zariski [15], § 13), we have

$$\deg(X \cdot (X+K(V))) = 2g(X) - 2, \qquad \deg(X' \cdot (X'+K(V))) = 2g(X') - 2,$$

where $g(X), g(X')$ denote the genera of X, X'. Since X and X' are numerically equivalent to each other, we see, from the above formulas, that $g(X) = g(X')$. Consequently we get the equality $p_a(X) = p_a(X')$ since the virtual arithmetic genus of a non-singular curve and its genus coincide. In the general case, let C be a hyperplane section of V. When m is sufficiently large, $\mathfrak{L}(X + mC)$ and $\mathfrak{L}(X' + mC)$ contain non-singular curves (Matsusaka [5], Lemmas 1, 2). Since all divisors in the same coset of $G(V)$ mod $G_l(V)$ have the same virtual arithmetic genus (Zariski [15], Lemma 4), we get the following equality by using the so-called modular property of p_a.

$$p_a(X) + p_a(mC) + p_a(mX \cdot C) = p_a(X') + p_a(mC) + p_a(mX' \cdot C).$$

(cf. Zariski [15], p. 582).

By the definition of p_a, we have $p_a(mX \cdot C) = \deg(mX \cdot C) - 1$ and $p_a(mX' \cdot C) = \deg(mX' \cdot C) - 1$. Therefore, we get the equality $p_a(X) = p_a(X')$.

PROPOSITION 3. *$G_n(V^2)/G_a(V^2)$ is a finite group.*

Proof. Let $\mathfrak{F}$ be a maximal total family on V such that it contains a divisor X satisfying the inequalities

$$\deg(X \cdot X) - p_a(X) + p_a(V) + 1 \geqq 0, \quad \deg(X) > \deg(K(V)).$$

When we take $\mathfrak{F}$ to be a maximal total family contained in $\mathfrak{A}(mX)$, where mC is a sufficiently high multiple of a hyperplane section C of V, the above condition is satisfied (cf. Th. 1 and Zariski [15], § 14). By the main theorem in Chow-v. d. Waerden [2], there is a finite number of maximal families of divisors $\mathfrak{F}_1 = \mathfrak{F}, \cdots, \mathfrak{F}_m$ in $\mathfrak{N}(X)$ such that any divisor in $\mathfrak{N}(X)$ is algebraically equivalent to a divisor in $\mathfrak{F}_i$ for some i, but no two of the $\mathfrak{F}_i$'s contain divisors algebraically equivalent to each other. Let X_i be a divisor in $\mathfrak{F}_i$ and assume that $X_1 = X$. By our assumption, X_i and X_j are algebraically equivalent to each other if and only if $i = j$. Let Z be any divisor numerically equivalent to 0. Then $X + Z$ and X are numerically equivalent to each other. Hence both have the same self-intersection number and the same virtual arithmetic genus by Prop. 2. Moreover, since $\deg(K(V)) < \deg(Z + X)$, it follows that $l(K(V) - X - Z) = 0$. Hence

$$\deg((X + Z) \cdot (X + Z)) - p_a(X + Z) + p_a(V) + 1 \geqq 0.$$

By the theorem of Riemann-Roch (Zariski [15], § 14), we see that $\mathfrak{L}^*(X + Z)$ contains a positive divisor X'. Hence X' must be algebraically equivalent to one of the X_i's. This proves that $X_i - X$ $(i = 1, \cdots, m)$ gives a complete set of representatives of $G_n(V)$ mod $G_a(V)$. Our proposition is thereby proved.

4.

THEOREM 4.[3] *Let V be a non-singular projective variety. Then $G_n(V)/G_a(V)$ is a finite group, and consequently it is the torsion group of V-divisors.*

Proof. Let W be a general surface on V and let r be the order of the group $G_n(W)/G_a(W)$. Assume that $G_n(V)/G_a(V)$ contains more than r elements and let $Z_1, \cdots, Z_{r+1}$ be $r+1$ representatives of $G_n(V) \bmod G_a(V)$ such that $Z_i \not\equiv Z_j \bmod _a(V)$ for $i \neq j$. We may assume that $Z_i \cdot W$ is defined. By Theorem 3, $\sum a_i Z_i \cdot W \equiv 0 \bmod G_a(W)$ implies $\sum a_i Z_i \equiv 0 \bmod G_a(V)$, but we must have a relation of the form $Z_i \cdot W \equiv Z_j \cdot W \bmod G_a(W)$ for a certain pair (i, j) of indices. This is impossible by our choice of the Z_i and consequently $G_n(V)/G_a(V)$ contains at most r elements. From this our theorem follows immediately.

Let $Z_1, \cdots, Z_s$ be a complete set of representatives of $G_n(V) \bmod G_a(V)$ and C be a hyperplane section of V. When m is sufficiently large, $\mathfrak{L}^*(Z_i + mC)$ contains a divisor $X_i \succ 0$ for every i. Let us assume that Z_i is algebraically equivalent to 0. Then X_1 is algebraically equivalent to mC. Thus we get the following corollary.

COROLLARY. *Let V be a projective non-singular variety and X be a positive V-divisor such that $\mathfrak{L}(X)$ determines an everywhere biregular birational transformation of V into a projective space. There is a positive integer m_0 with the following property: let $mX = Y_1, \cdots, Y_t$ be a complete set of representatives of $\mathfrak{N}(mX) \bmod G_a(V)$; then when $m \geqq m_0$, $Y_j - Y_1$, for $j = 1, \cdots, t$, is a complete set of representatives of $G_n(V) \bmod G_a(V)$.*

CHICAGO UNIVERSITY AND
OCHANOMIZU UNIVERISTY, TOKYO.

---

[3] The writer was informed that Mr. Y. Nakai obtained the same result.

REFERENCES.

[1] W. L. Chow, "Abstract theory of the Picard and Albanese varieties," to appear.

[2] ——— and B. L. van der Waerden, "Zur Algebraischen Geometrie IX," *Mathematische Annalen*, vol. 113 (1937), pp. 692-794.

[3] T. Matsusaka, "On the algebraic construction of the Picard variety," *Japanese Journal of Mathematics*, vol. 31 (1951), pp. 217-235.

[4] ———, "On the algebraic construction of the Picard variety II," *ibid.*, vol. 22 (1952), pp. 51-62.

[5] ———, "On the algebraic families of positive divisors," *Journal of the Mathematical Society of Japan*, vol. 5 (1953), pp. 115-136.

[6] ———, "Some theorems on Abelian varieties," *Natural Science Report*, Ochanomizu University, vol. 4 (1953), pp. 164-171.

[7] ———, "On the theorem of Castelnuovo-Enriques," *ibid.*, vol. 4 (1953), pp. 22-35.

[8] A. Néron, "Problèmes arithmétiques et géométriques rattachés à la notion du rang d'une courbe algébriques dans un corps," *Bulletin de la Société Mathématique de France*, vol. 80 (1952), pp. 101-166.

[9] ——— and P. Samuel, "La variété de Picard d'une variété Normale," *Annales de l'institut Fourier*, vol. 4 (1952), pp. 1-30.

[10] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[11] B. L. van der Waerden, "Zur Algebraischen Geometrie XIV," *Mathematische Annalen*, vol. 115 (1938), pp. 619-642.

[12] A. Weil, *Foundations of Algebraic Geometry*, American Mathematical Society Colloquium Publications, vol. 29 (1946).

[13] ———, "Variétés Abéliennes et Courbes Algébriques," *Actualités Scientifiques et Industrielles*, No. 1064 (1948).

[14] ———, "Sur les critères d'équivalence en géométrie algébriques," *Mathematische Annalen*, vol. 128 (1954), pp. 95-127.

[15] O. Zariski, "Complete linear systems on normal varieties and a generalization of a lemma of Enriques-Severi," *Annals of Mathematics*, vol. 55 (1952), pp. 552-592.

[16] ———, "Algebraic surfaces," *Ergebnisse der Mathematik und ihrer Grenzgebiete*, vol. 3, no. 5 (1935).

THE NILPOTENCE OF NIL SUBRINGS.*

By M. P. Drazin.

1. It is well known that, in any associative ring R with minimal condition on (say) left ideals, every nil left ideal is nilpotent (for the simplest known proof of this, due to R. Brauer, see [4, Theorem 13, p. 64]); more recently, Jacobson has shown ([5], and cf. also [4, Theorem 30, p. 71]) that every nil *subring* of R, besides also certain types of (nil) subsets not admitting the addition and multiplication of R, must be nilpotent. We recall also [4, Theorem 29, p. 71] that, at least in the presence of a two-sided identity element, the minimal condition on left ideals implies the maximal condition on these ideals.

Our main result in this note is that, in any associative ring with maximal condition on nilpotent subrings, every nil subring must in fact be nilpotent. Indeed, we establish the stronger result stated as Theorem 1 below; this may be compared with a result of Levitzki [6], who showed that, if R has maximal condition on both left and right ideals, then every nil subring of R is nilpotent (and that every nil *ideal* is nilpotent under a weaker, though more complicated, hypothesis; cf. also [7]).

In a concluding section, we establish some analogous results for Lie rings.

We note first a trivial lemma, which serves as a starting-point for our arguments in both the succeeding sections:

Lemma 1. *Let M be any given set, let $s \times t$ be any given binary operation in M, and let A be any subset of M closed under this operation. Then, for any given subsets T of A and U of M, either* (i) $A \leqq U$, *or* (ii) *we can find $a \in A$ and an infinite sequence $t_1, t_2, \cdots$ in T such that* $(\cdots((a \times t_1) \times t_2) \times \cdots) \times t_k \notin U$ $(k = 1, 2, \cdots)$, *or* (iii) *we can find $b \in A$ such that $b \notin U$ and $b \times t \in U$ for all $t \in T$.*

Proof. If (i) is false, then we can certainly choose $a \in A$ with $a \notin U$. Then we have the following inductive method of constructing a sequence $t_1, t_2, \cdots$ satisfying (ii), which method can break down at some stage only if (iii) holds: supposing, for a given positive integer k, that $t_1, \cdots, t_{k-1}$

* Received July 30, 1956.

are already defined so that $b = (\cdots (a \times t_1) \times t_2 \cdots) \times t_{k-1} \notin U$, then, since $T \leqq A$ and A is closed, we have $b \in A$, and so, if b does not satisfy (iii), we can choose a suitable t_k, and so on.

2. In this section we take M to be an associative ring R (possibly considered as a ring with operators) and, given any subset C of R, we write C^* to denote the subring generated by C. We also now require, for each pair $s, t \in R$, that $s \times t$ should be of the form

$$s \times t = st + xs + y,$$

where both $x = x(s,t)$ and $y = y(s,t)$ are in the subring $\{t\}^*$ of R generated by t; and, when we speak of a *closed* subset A of R, we shall mean that $s \times t \in A$ whenever both $s, t \in A$.

LEMMA 2. *Given any ring R, any closed subset A of R and an arbitrary subset T of A, then either* (1) $A^* = T^*$, *or* (2) *we can find $a \in A$ such that $T^{*i}a + aT^{*i} \neq 0$ $(i = 1, 2, \cdots)$, or* (3) *we can find $b \in A$ such that $b \notin T^*$ and, for each $t \in T$, $bt \in T^* + T^*b$.*

Proof. We show that, on taking $U = T^*$ in Lemma 1, then (i), (ii), (iii) respectively imply (1), (2), (3). For, if (i) holds, i.e., if $A \leqq T^*$, then of course $A^* \leqq T^*$, while also (since $A \geqq T$) $A^* \geqq T^*$, so (1) follows. Next, for any $t_1, \cdots, t_k \in T$, clearly $(\cdots ((a \times t_1) \times t_2) \times \cdots) \times t_k$ is, modulo T^*, a sum of terms of the form $z_1 \cdots z_j a z_{j+1} \cdots z_k$ with each $z_i \in T^*$, so that $(\cdots ((a \times t_1) \times t_2) \times \cdots) \times t_k \in T^* + \sum_{j=0}^{k} T^{*j} a T^{*k-j}$; if (ii) holds, i.e., if the element on the left is *not* in T^*, then certainly $\sum_{j=0}^{k} T^{*j} a T^{*k-j} \neq 0$ $(k = 1, 2, \cdots)$, which gives (2) on taking $k = 2i - 1$. Finally, (iii) gives $b \notin T^*$ and, for any $t \in T$, we have $bt = b \times t - y - xb$, where $b \times t$, $x, y \in T^*$.

Lemmas 1 and 2 are both implicit in Jacobson's paper [5], though he considered only "products" of the more special form $s \times t = st + xs$, with $x = x(s,t)$ an *operator multiple* of t. It is, of course, easy to deduce from (3), as Jacobson did, that $bT^* \leqq T^* + T^*b$; however, Jacobson's own later argument uses only the fact that bT^* is contained in the right ideal of R generated by T, and this is an obvious consequence of (3).

THEOREM 1. *Let R be any given associative ring with maximal condition on nilpotent subrings, and A any closed subset of R. Then, if A is nil (i.e. has all its elements nilpotent), it generates a nilpotent subring of R.*

Proof. We first apply our hypothesis about R to select, from among those subsets B of A which generate nilpotent subrings B^* of R (and certainly such B exist provided that A is not empty), a subset T of A such that T^* is maximal in the class of all subrings B^* arising in this way. Since T^* is nilpotent, it is enough to show that (1) of Lemma 2 holds; and, since the nilpotence of T^* contradicts (2), we need consequently only prove (3) false, i. e., show that no element b of A can have the stated properties.

To do this, let b be as in (3), and let S denote the subring generated by T together with b, so that (since $b \notin T^*$) S contains T^* properly; then, by the maximality of T^* among all the B^*, it will suffice, in order to obtain our desired contradiction, to show that S is itself a B^*, i. e. (since S is certainly generated by a subset of A), that S is nilpotent.

Since A is nil and $b \in A$, we have $b^m = 0$ for some integer $m \geqq 2$. Now, for each positive integer n, every element of S^{mn} is a linear combination of monomials $g = c_1 \cdots c_r$, where $r \geqq mn$ and, for each i, either $c_i = b$ or $c_i \in T$. Also a non-zero g can have no more than $m-1$ consecutive factors b occurring anywhere in it, so, if q denotes the total number of factors from T occurring, then g can be non-zero only if

$$q \geqq \frac{r-q}{m-1} - 1,$$

so that $q \geqq (r-m+1)/m \geqq (mn-m+1)/m$, i. e. $q \geqq n$. In other words, at least n factors from T must occur in any non-zero monomial $g \in S^{mn}$, and so, by use of (3), we can express every element of S^{mn} as a linear combination of products $d_1 \cdots d_q b^j$, where $q \geqq n$, each $d_i \in T^*$ and $0 \leqq j \leqq m-1$, i. e.

$$S^{mn} \leqq T^{*n} + \sum_{j=1}^{m-1} T^{*n} b^j \qquad (n = 1, 2, \cdots).$$

Hence, since T^* is nilpotent, so is S and the theorem follows.

3. Arguments analogous to most of those in the preceding section can be carried through for Lie rings. This can be done in two ways, by applying Lemma 1 with M taken to be either the given Lie ring itself or the (associative) set of (say) right multiplications of the given ring. However, the results obtainable by the former method seem to be the more interesting, and we shall not discuss the other possible approach further.

From now on, we suppose that we are given a Lie ring L and an operation $s \times t$ in L such that, for each pair $s, t \in L$,

$$s \times t = st + y,$$

where $y = y(s,t)$ is some integral or operator *multiple* of t (and where st is of course now a Lie product). Closure will, naturally, refer to this operation, while C^* will now denote the Lie subring of L generated by a given subset C of L. Corresponding to Lemma 2 above, we now have

LEMMA 3. *Given any Lie ring L, any closed subset A of L and an arbitrary subset T of A, then either* (1′) $A^* = T^*$, *or* (2′) *we can find $a \in A$ and an infinite sequence $t_1, t_2 \cdots$ in T such that* $(\cdots((at_1)t_2)\cdots)t_k \notin T^*$ $(k = 1, 2, \cdots)$, *or* (3′) *we can find $b \in A$ such that $b \notin T^*$ and $bT^* \leqq T^*$.*

Proof. We apply Lemma 1 with $U = T^*$, much as before. We deduce (1′) from (i) exactly as in Lemma 2, and this time it is even easier to deduce (2′) from (ii). Finally, (iii) gives $bt \in T^*$ for every $t \in T$, whence the Jacobi identity, together with a straightforward induction on the degrees of the T-monomials involved, gives (3′).

In order to be able to state our next theorem concisely, we introduce some notation and terminology. Given any elements $a_1, a_2, \cdots$ of L, then any product $a_1 a_2 \cdots a_k$ written without parentheses is to be understood as standing for the corresponding left-normed Lie product $(\cdots((a_1a_2)a_3)\cdots)a_k$; and, more generally, given subsets $A_1, A_2, \cdots$ of L, we write $A_1A_2 \cdots A_k$ to denote the set of all products of the form $a_1a_2 \cdots a_k$ with each $a_i \in A_i$. With these conventions, we can use Bc^k to denote the set of all $(\cdots((zc)c)\cdots)c$ as z runs through B (with just k factors c); similarly, BC^k will denote the set of all $(\cdots((za_1)a_2)\cdots)a_k$ as z runs through B and the a_i run independently through C. We shall call an element c of L *nilpotent on* L if $Lc^k = 0$ for some integer $k = k(c)$, and shall call a subset C of L nilpotent on L if $LC^k = 0$ for some $k = k(C)$; if every element of a subset C of L is nilpotent on L (the implied k's being not necessarily bounded) then we shall call C *nil on* L.

We can now apply Lemma 3, and arguments parallel to those used in proving Theorem 1, to derive

THEOREM 2. *Let L be a given Lie ring with maximal condition on nilpotent subrings (nilpotent being here interpreted in the ordinary Lie sense) and A any closed subset of L. Then, if A is nil on L, the subring of L generated by A is nilpotent on L (and, a fortiori, nilpotent).*

Proof. We first apply the hypothesis on L to select, from among those subsets B of A which generate subrings B^* of L which are nilpotent on L, a subset T of A such that T^* is maximal in the class of all subrings B^* arising in this way. As before, it is enough to show that (1′) of Lemma 3

holds; and, since the nilpotence of T^* on L rules out (2′), we need only prove (3′) false.

Suppose then, by way of contradiction, that A contains an element b satisfying (3′) and let S denote the subring of L generated by T^* together with b, so that S contains T^* properly; then, by the maximality of T^* among the B^*, it is enough to show that S is a B^*, i.e., that S is nilpotent on L.

Since A is nil on L and $b \in A$, we have $Lb^m = 0$ for some $m \geqq 2$, and, since $bT^* = T^*b \leqq T^*$, clearly $S = T^* + Fb$, where F denotes the ring of integers (or any commutative ring of admissible operators). Next, for any $u \in L$, $v \in T^*$, we have, by the Jacobi identity and (3′), that $ubv = uvb + u(bv)$, where $bv \in T^*$, so that

(3″) $$ubv - uvb \in uT^* \textit{ whenever } u \in L, v \in T^*.$$

Now, for any positive integer n, since $S = T^* + Fb$, clearly every element of LS^{mn} is a linear combination of Lie monomials $g = zc_1c_2 \cdots c_{mn}$, where $z \in L$ and, for each i, either $c_i = b$ or $c_i \in T^*$. Also a non-zero g can have no more than $m - 1$ consecutive factors b occurring in it anywhere, so, if q denotes the total number of factors from T^* occurring, then, as before,

$$q \geqq (mn - q)/(m - 1) - 1,$$

i.e., $q \geqq n$. In other words, at least n factors from T^* must occur in any non-zero monomial g, and so, by use of (3″), we can express every element of LS^{mn} as a linear combination of products $zd_1 \cdots d_q b^j$ with $q \geqq n$, each $d_i \in T^*$ and $0 \leqq j \leqq m - 1$, i.e.

$$LS^{mn} \leqq LT^{*n} + \sum_{j=1}^{m-1} LT^{*n} b^j \qquad (n = 1, 2, \cdots).$$

Hence, since T^* is nilpotent on L, so is S and the theorem follows.

Theorem 2 generalizes a result of Zorn [8], who considered only the case in which $s \times t = st$ and $A = L$.

We conclude with two other results, which, though little short of obvious, seem worth putting on record for comparison with Theorem 2 (cf. also [1], [2], [3]):

THEOREM 3. *Let L be a Lie ring with maximal condition on Lie ideals and having characteristic zero. Then, if to each $z \in L$ there corresponds a positive integer $k(z)$ such that $zc^{k(z)} = 0$ for every $c \in L$, we can find a fixed integer k such that $zc^k = 0$ for all $z, c \in L$.*

Proof. For each positive integer j, let X_j denote the set of all $x \in L$

such that $xy^j = 0$ for all $y \in L$. Then it can be shown that each X_j is an ideal of L; we shall not go into the (straightforward but not quite trivial) proof of this fact in detail here, but see e.g. [3, Lemma 4], where a more general result is established. Also clearly $X_j \leqq X_{j+1}$ $(j = 1, 2, \cdots)$, and so, by the maximal condition, there is an integer k such that X_k contains all the other X_j. Thus, for each $z \in L$, we have $z \in X_{k(z)} \leqq X_k$, i.e., $zc^k = 0$ for all $z, c \in L$.

In a precisely similar way, we find

THEOREM 4. *Let L be a Lie ring with maximal condition on Lie ideals and having characteristic zero, and suppose that, to each $z \in$ L, there corresponds a positive integer $k(z)$ such that $zL^{k(z)} = 0$. Then L must in fact be nilpotent.*

TRINITY COLLEGE, CAMBRIDGE.

REFERENCES.

[1] M. P. Drazin, "Engel rings and a result of Herstein and Kaplansky," *American Journal of Mathematics*, vol. 77 (1955), pp. 895-913.

[2] K. W. Gruenberg, "Two theorems on Engel groups," *Proceedings of the Cambridge Philosophical Society*, vol. 49 (1953), pp. 377-380.

[3] P. J. Higgins, "Lie rings satisfying the Engel condition," *Proceedings of the Cambridge Philosophical Society*, vol. 50 (1954), pp. 8-15.

[4] N. Jacobson, *The Theory of Rings* (American Mathematical Society, 1943).

[5] ———, "Une généralisation du théorème d'Engel," *Comptes Rendus des Séances de l'Académie des Sciences*, vol. 234 (1952), pp. 579-581.

[6] J. Levitzki, "Solution of a problem of G. Koethe," *American Journal of Mathematics*, vol. 67 (1945), pp. 437-442.

[7] ———, "On multiplicative systems," *Compositio Mathematica*, vol. 8 (1951), pp. 76-80.

[8] M. Zorn, "On a theorem of Engel," *Bulletin of the American Mathematical Society*, vol. 43 (1937), pp. 401-404.

A CHARACTERIZATION OF THE LEBESGUE AREA.*

By Christoph J. Neugebauer.

Introduction. The characterization of the Lebesgue area as a functional Φ defined on a certain class of continuous mappings has attracted a great deal of attention. The conditions that are imposed upon a functional Φ in this paper (see Section 3) are essentially those listed in L. Cesari [2; 7.5]. Let $\mathfrak{T}$ be the class of all continuous mappings (T, A) from an admissible subset A of E_2 into E_3 (see Section 1), and let $L(T, A)$ be the Lebesgue area of (T, A). A subclass $\mathfrak{T}'$ of $\mathfrak{T}$ is considered which consists of all mappings (T, A) in $\mathfrak{T}$ admitting an *elementary shrinking approach* (see Section 4), and it is shown that $\mathfrak{T}'$ is the class of mappings on which each functional Φ satisfying the conditions of Section 3 agrees with the Lebesgue area.

1. Some definitions. We will be concerned with the collection of *admissible* subsets A of the Euclidean plane E_2. By L. Cesari [2; 5.1] this collection comprises (a) all open subsets of E_2, (b) all finite unions of disjoint closed finitely connected Jordan regions, and (c) all open subsets of sets described in (b). The interior of a set A will be denoted by A^0, and the closure of A will be designated by $\bar{A}$. The distance between two point p', p'' of a Euclidean space will be abbreviated by $|p' - p''|$.

Let $\mathfrak{T}$ be the class of all continuous mappings (T, A) from an admissible sets $A \subset E_2$ into the Euclidean three space E_3. The following statements are needed.

(i) A sequence of mappings (T_n, A_n) in $\mathfrak{T}$ is said to *converge* to a mapping (T, A) in $\mathfrak{T}$ provided (1) $A_n \subset A_{n+1} \subset A$, $A_n^0 \uparrow A^0$, (2) $d(T, T_n, A_n) \to 0$ as $n \to \infty$, where $d(T, T_n, A_n) = \text{l.u.b.}\,|T(w) - T_n(w)|$, $w \in A_n$ (see [2; 5.3]).

(ii) Let R be the generic notation for the interior of a finite union of disjoint finitely connected Jordan regions. A mapping (T, R) in $\mathfrak{T}$ will be termed *elementary* provided (a) T admits of a continuous extension to $\bar{R}$, (b) there is a quasi-linear mapping Fréchet equivalent to $(T, \bar{R})$. For the concept of Fréchet equivalence see [2; 31.2].

* **Received March 5, 1956; revised August 17, 1956.**

2. Some preliminary results. In this article we will discuss some lemmas which are concerned with Lipschitzian mappings F of constant one from E_3 into E_3. The class of those mappings F will be denoted by $\mathfrak{L}$. The lemma (i) below is a special case of a theorem in E. J. Mickle [5].

(i) LEMMA. *Let B be a subset of E_3 and let F be a Lipschitzian mapping of constant one from B into E_3. Then F can be extended to a Lipschitzian mapping of constant one from E_3 into E_3.*

(ii) LEMMA. *Let (T,A) and (T',A) be two mappings in $\mathfrak{T}$ such that for each w, w' in A, $|T'(w)-T'(w')| \leqq |T(w)-T(w')|$. Then there exists a mapping F in $\mathfrak{L}$ such that $(T',A)=(FT,A)$.*

Proof. Let γ be a set in A on which T is constant. Then by hypothesis T' is also constant on γ. Therefore, the mapping $F'=T'T^{-1}$ is a single-valued transformation from $T(A)$ onto $T'(A)$. We assert next that $|F'(p)-F'(p')| \leqq |p-p'|$, $p, p' \in T(A)$. For $p, p' \in T(A)$ let w, w' be two points in A for which $T(w)=p$, $T(w')=p'$. Then

$$\begin{aligned} |F'(p)-F'(p')| &= |T'T^{-1}(p)-T'T^{-1}(p')| \\ &= |T'(w)-T'(w')| \leqq |T(w)-T(w')| = |p-p'|. \end{aligned}$$

By (i), F' admits an extension F to E_3 satisfying the desired properties.

(iii) LEMMA. *Let (T_0,A_0) be a fixed mapping in $\mathfrak{T}$ and let (T_n,A_n), $n=1,2,\cdots$, be a sequence of mappings in $\mathfrak{T}$ satisfying (1) $(T_n,A_n)\rightarrow(T,A)$, $(T,A)\in\mathfrak{T}$, $A\subset A_0$, (2) for each n, there is a mapping $F_n\in\mathfrak{L}$ such that $(T_n,A_n)=(F_nT_0,A_n)$. Then there exists a mapping $F\in\mathfrak{L}$ with the property that $(T,A)=(FT_0,A)$.*

Proof. Let w, w' be any two points in A and let $\{w_i\}$, $\{w_i'\}$ be two sequences in A^0 such that $w_i\rightarrow w$, $w_i'\rightarrow w'$. Since by 1(i), $A_n\subset A_{n+1}\subset A$, $A^0{}_n\uparrow A^0$, we may choose integers $n_1<n_2<\cdots<n_i<\cdots$ such that w_i, w_i' are both in $A^0{}_{n_i}$. Now, since $T(w_i)\rightarrow T(w)$, $T(w_i')\rightarrow T(w')$, and since in view of 1(i), $|T(w_i)-T_{n_i}(w_i)|\rightarrow 0$, $|T(w_i')-T_{n_i}(w_i')|\rightarrow 0$ as $i\rightarrow\infty$, we conclude that $T_{n_i}(w_i)\rightarrow T(w)$, $T_{n_i}(w_i')\rightarrow T(w')$. Moreover, the continuity of T_0 implies $T_0(w_i)\rightarrow T_0(w)$, $T_0(w_i')\rightarrow T_0(w')$.

Let $\epsilon>0$ be given. Then we can determine an integer $J>0$ such that for $i>J$,

$$\begin{gathered} |T(w)-T_{n_i}(w_i)|<\epsilon/3, \qquad |T(w')-T_{n_i}(w_i')|<\epsilon/3, \\ |T_0(w_i)-T_0(w_i')|<|T_0(w')-T_0(w)|+\epsilon/3. \end{gathered}$$

Since $T_{n_i}(w_i) = F_{n_i}T_0(w_i)$, $T_{n_i}(w_i') = F_{n_i}T_0(w_i')$, there follows for $i > J$,

$$|T(w) - T(w')| \leqq |T(w) - T_{n_i}(w_i)| + |T_{n_i}(w_i) - T_{n_i}(w_i')|$$
$$+ |T_{n_i}(w_i') - T(w')| \leqq |T(w) - T_{n_i}(w_i)| + |T_0(w_i) - T_0(w_i')|$$
$$+ |T_{n_i}(w_i') - T(w')| < |T_0(w) - T_0(w')| + \epsilon.$$

Since $\epsilon > 0$ was arbitrary, $|T(w) - T(w')| \leqq |T_0(w) - T_0(w')|$. By (ii) the proof is complete.

3. Class $\mathfrak{T}^*$. Let $\mathfrak{F}$ be the class of all functionals $\Phi(T, A)$ defined for $(T, A) \in \mathfrak{T}$ satisfying the following conditions:

(a) $\Phi(T, A) \geqq 0$ for $(T, A) \in \mathfrak{T}$.

(b) $\Phi(T, A)$ is lower semi-continuous, i.e., if $(T_n, A_n) \to (T, A)$, then $\Phi(T, A) \leqq \liminf_{n\to\infty} \Phi(T_n, A_n)$.

(c) $\Phi(T, A)$ satisfies the Kolmogoroff principle, i.e., for $F \in \mathfrak{L}$, $\Phi(FT, A) \leqq \Phi(T, A)$.

(d) $\Phi(T, A)$ is monotone, i.e., for $(T, A) \in \mathfrak{T}$ and A' an admissible subset of A, $\Phi(T, A') \leqq \Phi(T, A)$.

(e) For (T, R) an elementary mapping (see Section 1(ii)), $\Phi(T, R) = L(T, R)$.

Remark. The Lebesgue area $L(T, A)$ satisfies the above conditions and hence is a functional in $\mathfrak{F}$ (see [2]). For each $\Phi \in \mathfrak{F}$ and each $(T, A) \in \mathfrak{T}$ we have $\Phi(T, A) \leqq L(T, A)$ (see [2; 5.12]).

For every $\Phi \in \mathfrak{F}$ let $\mathfrak{T}(\Phi)$ be the class of mappings $(T, A) \in \mathfrak{T}$ for which $\Phi(T, A) = L(T, A)$. Finally, let $\mathfrak{T}^* = \cap\, \mathfrak{T}(\Phi)$, $\Phi \in \mathfrak{F}$. In view of (e), $\mathfrak{T}^*$ contains all elementary mappings.

4. Class $\mathfrak{T}'$. *Definition.* A mapping $(T, A) \in \mathfrak{T}$ is said to satisfy the *condition* (s) provided for every $\epsilon > 0$ there exists an elementary mapping (T', R) (see Section 1(ii)) with $R \subset A$ and

(1) $\quad |T'(w) - T'(w')| \leqq |T(w) - T(w')|, \qquad w, w' \in R$

(2) $\quad L(T, A) - L(T', R) < \epsilon$, if $L(T, A) < \infty$, $L(T', R) > \epsilon^{-1}$ if $L(T, A) = +\infty$.

It may be of interest to note that (1) does not imply that (T', R) approximates (T, A). It is only required that $L(T', R)$ approximates $L(T, A)$.

Let us denote by $\mathfrak{T}'$ the class of all mappings (T, A) in $\mathfrak{T}$ which satisfy the condition (s). Concerning the class $\mathfrak{T}'$ we have the following two lemmas.

(i) Lemma. *The class $\mathfrak{T}'$ contains all elementary mappings as well as all mappings (T, A) for which $L(T, A) = 0$.*

Proof. The first statement is obvious, and for the second it suffices to let (T', R), $R \subset A$, be constant on R.

(ii) Lemma. *If (T, A) is in $\mathfrak{T}'$, then (T, A^0) is also in $\mathfrak{T}'$.*

Proof. Since (T, A) is in $\mathfrak{T}'$ there is, for $\epsilon > 0$ given, an elementary mapping (T', R), $R \subset A$, such that (1) and (2) are satisfied. Since (T', R) is elementary, the set R is an open subset of E_2 (see Section 1(ii)). Hence $R \subset A^0$, and since $L(T, A) = L(T, A^0)$, the mapping (T, A^0) is in $\mathfrak{T}'$.

5. Main result. We are now ready to prove

Theorem. $\mathfrak{T}^* = \mathfrak{T}'$.

Proof. In view of Section 3 we have for every $\Phi \in \mathfrak{F}$ and for every $(T, A) \in \mathfrak{T}$ the inequality $\Phi(T, A) \leqq L(T, A)$. We will first prove that $\mathfrak{T}^* \supset \mathfrak{T}'$. If we deny this inclusion, we have a functional $\Phi \in \mathfrak{F}$ and a mapping (T, A) in $\mathfrak{T}'$ such that $\Phi(T, A) < L(T, A)$. Since (T, A) satisfies the condition (s), there is an elementary mapping (T', R), $R \subset A$, such that $L(T', R) > \Phi(T, A)$ and

$$(1) \qquad |T'(w) - T'(w')| \leqq |T(w) - T(w')|, \qquad w, w' \in R.$$

In view of the conditions 3(d), (e), we infer that

$$(2) \qquad \Phi(T', R) = L(T', R) > \Phi(T, A) \geqq \Phi(T, R).$$

However, from 2(ii) and 3(c) we deduce by (1) $\Phi(T', R) \leqq \Phi(T, R)$, a contradiction with (2). Therefore, $\mathfrak{T}^* \supset \mathfrak{T}'$.

6. To prove the complementary inclusion $\mathfrak{T}^* \subset \mathfrak{T}'$, let us assume that there is a mapping (T_0, A_0) in $\mathfrak{T}^*$ which is not in $\mathfrak{T}'$. From 4(i) we have that $L(T_0, A_0) > 0$. There exists now a number $\lambda_0 \geqq 0$ with $L(T_0, A_0) > \lambda_0$ such that for every elementary mapping (T', R), $R \subset A_0$, for which $|T'(w) - T'(w')| \leqq |T_0(w) - T_0(w')|$, $w, w' \in R$, we have $L(T', R) \leqq \lambda_0$.

Let $\mathfrak{K}_0$ be the class of mappings (T, A') in $\mathfrak{T}$ such that (1) $A' \subset A_0$, (2) there exists a mapping $F \in \mathfrak{L}$ such that $(T, A') = (FT_0, A')$, (3) $L(T, A') > \lambda_0$. Finally, let $\mathfrak{K}_0'$ be the class of mappings $(T, A) \in \mathfrak{T}$ for

which there exists a sequence $(T_n, A_n) \in \mathfrak{K}_0$ such that $(T_n, A_n) \to (T, A)$ and $L(T, A) > \lambda_0$. Note that $\mathfrak{K}_0 \subset \mathfrak{K}_0'$, and if A_0 is compact then $\mathfrak{K}_0 = \mathfrak{K}_0'$.

7. In this paragraph we will prove some lemmas concerning the class $\mathfrak{K}_0'$.

(i) LEMMA. *If $(T, A) \in \mathfrak{K}_0'$, then $(T, A^0) \in \mathfrak{K}_0$.*

Proof. We have a sequence of mappings $(T_n, A_n) \in \mathfrak{K}_0$ such that $(T_n, A_n) \to (T, A)$ and $L(T, A) > \lambda_0$. By 1(i), $A_n \subset A_{n+1} \subset A$, $A_n{}^0 \uparrow A^0$. Since also $A_n \subset A_0$, $n = 1, 2, \cdots$, the set A^0 is a subset of A_0. For each n, there is a mapping $F_n \in \mathfrak{L}$ for which $(T_n, A_n{}^0) = (F_n T_0, A_n{}^0)$. Since clearly $(T_n, A_n{}^0) \to (T, A^0)$, we have by 2(iii) a mapping $F \in \mathfrak{L}$ such that $(T, A^0) = (FT_0, A^0)$. Since, finally, $L(T, A^0) = L(T, A) > \lambda_0$, we infer from the definition of $\mathfrak{K}_0$ that $(T, A^0) \in \mathfrak{K}_0$.

(ii) LEMMA. *$\mathfrak{K}_0'$ contains no elementary mappings.*

Proof. If (T, R) is an elementary mapping in $\mathfrak{K}_0'$, then from 1(ii), $R = R^0$. Thus by (i), $(T, R) \in \mathfrak{K}_0$. But then from the definition of $\mathfrak{K}_0$ we have a mapping $F \in \mathfrak{L}$ such that $(T, R) = (FT_0, R)$ and $L(T, R) > \lambda_0$. In view of Section 6 this is impossible and hence $\mathfrak{K}_0'$ contains no elementary mappings.

(iii) LEMMA. *Let (T, A) be in $\mathfrak{K}_0'$ and let A' be an admissible subset of A. Assume there is a mapping $F \in \mathfrak{L}$ such that $L(FT, A') > \lambda_0$. Then $(FT, A') \in \mathfrak{K}_0'$.*

Proof. We have a sequence (T_n, A_n) in $\mathfrak{K}_0$ such that $(T_n, A_n) \to (T, A)$. Since the sets $A_n' = A_n \cap A'$ satisfy the properties $A_n' \subset A_{n+1}' \subset A'$, $A_n'^0 \uparrow A'^0$, we have that $(FT_n, A_n'^0) \to (FT, A')$. From $L(FT, A') > \lambda_0$, we have as a consequence of the lower semi-continuity of the Lebesgue area, $L(FT_n, A_n'^0) > \lambda_0$ for n large. Thus $(FT_n, A_n'^0)$ is in $\mathfrak{K}_0$ for n large, and the lemma follows.

(iv) LEMMA. *Let (T_n, A_n) be a sequence in $\mathfrak{K}_0'$ such that $(T_n, A_n) \to (T, A)$. Then, if $L(T, A) > \lambda_0$, the mapping (T, A) is in $\mathfrak{K}_0'$.*

Proof. From (i), $(T_n, A_n{}^0)$ is in $\mathfrak{K}_0$ for each n, and from 1(i), $(T_n, A_n{}^0) \to (T, A)$. Thus, (T, A) is in $\mathfrak{K}_0'$.

8. Define a functional $\Phi(T, A)$ for $(T, A) \in \mathfrak{T}$ as follows: $\Phi(T, A) = \lambda_0$ if $(T, A) \in \mathfrak{K}_0'$, and $\Phi(T, A) = L(T, A)$ otherwise. We will verify now that

$\Phi(T,A)$ satisfies the conditions of Section 3. Since 3(a) is obvious, we will prove that

(b) $\Phi(T,A)$ is lower semi-continuous.

Proof. Let (T_n, A_n) be a sequence of mappings in $\mathfrak{T}$ which converges to (T,A). Then $L(T,A) \leqq \liminf L(T_n, A_n)$ as $n \to \infty$. Hence, if $L(T,A) \leqq \lambda_0$, then $\Phi(T,A) \leqq \liminf \Phi(T_n, A_n)$, from the definition of $\Phi(T,A)$. Assume now that $L(T,A) > \lambda_0$. Then there exists an integer $N > 0$ such that for $n > N$, $L(T_n, A_n) > \lambda_0$. Hence for $n > N$, $\lambda_0 \leqq \Phi(T_n, A_n) \leqq L(T_n, A_n)$. If $(T,A) \in \mathfrak{K}_0'$, we infer that $\Phi(T,A) \leqq \liminf \Phi(T_n, A_n)$. If (T,A) is not in $\mathfrak{K}_0'$, then by 7(iv), only a finite number of the (T_n, A_n) can be in $\mathfrak{K}_0'$. Thus $\Phi(T,A) \leqq \liminf \Phi(T_n, A_n)$.

(c) $\Phi(T,A)$ satisfies the Kolmogoroff principle.

Proof. Let F be in $\mathfrak{L}$. If (T,A) is not in $\mathfrak{K}_0'$, then clearly $\Phi(FT,A) \leqq L(FT,A) \leqq L(T,A) = \Phi(T,A)$. Assume now that (T,A) is in $\mathfrak{K}_0'$. If $L(FT,A) > \lambda_0$, we conclude from 7(iii) that (FT,A) is in $\mathfrak{K}_0'$, and hence $\Phi(FT,A) = \Phi(T,A)$. If $L(FT,A) \leqq \lambda_0$, then clearly $\Phi(FT,A) = L(FT,A) \leqq \lambda_0 = \Phi(T,A)$.

(d) $\Phi(T,A)$ is monotone.

Proof. This is a ready consequence of the definition of Φ and $\mathfrak{K}_0'$.

(e) $\Phi(T,R) = L(T,R)$ if (T,R) is elementary.

Proof. If (T,R) is elementary, then it follows from 7(ii) that (T,R) is not in $\mathfrak{K}_0'$. Therefore, (e) is a consequence of the definition of Φ.

Under the assumption that there is a mapping (T_0, A_0) in $\mathfrak{T}^*$ not in $\mathfrak{T}'$ there can be exhibited a functional $\Phi \in \mathfrak{F}$ such that $\Phi(T_0, A_0) < L(T_0, A_0)$. But this contradicts the definition of $\mathfrak{T}^*$, and therefore $\mathfrak{T}^* \subset \mathfrak{T}'$. With the inclusion established in Section 5, the proof of the main result is complete.

9. Lemma. *For $\Phi \in \mathfrak{F}$ and $(T,A) \in \mathfrak{T}^*$ we have $\Phi(T,A^0) = \Phi(T,A)$.*

Proof. From 5, (T,A) is in $\mathfrak{T}'$ and from 4(ii), (T,A^0) is in $\mathfrak{T}'$. Thus $\Phi(T,A^0) = L(T,A^0) = L(T,A) = \Phi(T,A)$.

10. A definite relation between the classes $\mathfrak{T}'$ and $\mathfrak{T}$ is not known to the writer. A solution of this problem would answer the question whether or not the conditions listed in Section 3 suffice to characterize the Lebesgue area. In this connection the following comments are in order. The condition 3(e)

is concerned with Fréchet equivalence. If one were to modify the condition 3(e) to (e′) by replacing Fréchet equivalence by Lebesgue equivalence in 3(e), then an example of a functional satisfying the conditions 3(a), (b), (c), (d) and (e′) can be exhibited which does not agree with the Lebesgue area. An example of such a functional will be pubilshed elsewhere.

PURDUE UNIVERSITY.

REFERENCES.

[1] J. Cecconi, "Sull' area di Peano e sulla definizione assiomatica dell' area di una superficie," *Rendiconti del Seminario Matematico della Univeristà di Padova*, vol. 20 (1951), pp. 307-314.

[2] L. Cesari, *Surface Area*, Princeton University Press, 1956.

[3] ———, "L'area di Lebesgue come una misura," *Rendiconti di Matematica e delle sue Applicazioni*, Roma, (5) 14, 1955, pp. 655-673.

[4] G. Scorza Dragoni, "Sulla definizione assiomatica dell' area di una superficie," *Rendiconti del Seminario Matematico della Università di Padova*, vol. 5 (1946), pp. 8-24.

[5] E. J. Mickle, "On the extension of a transformation," *Bulletin of the American Mathematical Society*, vol. 55 (1949), pp. 160-164.

[6] M. Pagni, "Sulla definizione dell' area di una superficie per via assiomatica," *Rendiconti del Seminario Matematico della Università di Padova*, vol. 19 (1950), pp. 303-316.

[7] T. Radó, *Length and Area*, American Mathematical Society Colloquium Publications, vol. 30 (1948).

[8] E. Silverman, "Definition of Lebesgue area for surfaces in metric spaces,' *Rivista di Matematica della Università di Parma*, vol. 2 (1951), pp. 47-76.

[9] G. Stampacchia, "Sulla definizuone assiomatica dell' area di una superficie rettificabile," *Rendiconti Accademia Nazionale di Lincei*, vol. 2 (1947), pp. 542-546.

[10] G. Zwirner, "Sulla definizione d'area di una superficie," *Istituto Veneto di Scienze, Lettere ed Arti Venezia*, vol 97, 2 (1937-38), pp. 409-416.

WEAKLY STANDARD RINGS.*

By R. L. San Soucie.

1. Introduction. Generalizing the standard algebras of Albert (see [1], p. 576), Kleinfeld [5] has called a ring *accessible* if the following identities hold:

$$(x,y,z)+(z,x,y)-(x,z,y)=0, \tag{1.1}$$

$$((w,x),y,z)=0, \tag{1.2}$$

where the associator (x,y,z) and the commutator (w,x) are defined by

$$(x,y,z)=xy\cdot z-x\cdot yz, \qquad (w,x)=wx-xw. \tag{1.3}$$

The substitution of x for z in (1.1) gives the relation

$$(x,y,x)=0, \tag{1.4}$$

so that accessible rings are *flexible* (see [1], p. 561). A linearization of the flexible law yields the identity

$$(x,y,z)=-(z,y,x), \tag{1.5}$$

valid in any flexible ring. Hence it follows from (1.2), (1.5) and (1.1) that the following identity also holds in an accessible ring:

$$(w,(x,y),z)=0. \tag{1.6}$$

We propose, therefore, to call a ring, R, *weakly standard* [1] if R is flexible and if identities (1.2) and (1.6) hold in R. Thus the accessible rings of Kleinfeld, as well as the standard algebras of Albert, are automatically

* Received July 10, 1956.

[1] Kleinfeld's analogue of our Theorem 2 was announced by him in an abstract which appeared in the January 1956 *Bulletin* and it was this result of his, as published, which called our attention to these matters. We then generalized the concept of accessible ring to that of weakly standard ring, and proved Theorems 1, 2, and 3, as well as a weaker version of Theorem 4, requiring also the absence of non-zero nilpotent elements. Subsequent communication with Kleinfeld informed us that his results, for accessible rings, also included the prime, primitive and semi-simple cases, although not included in his abstract. Hence our work on Theorems 1 and 3 was independent. The author hereby acknowledges this communication with Kleinfeld and notes, with thanks, that Kleinfeld provided him with a copy of his manuscript of [5], prior to its publication.

weakly standard. On the other hand, we shall give an example later in the paper of a weakly standard ring which is not accessible.

The results obtained parallel those of Kleinfeld for accessible rings, but the method is different. We first show that a prime ring is weakly standard if and only if it is either associative or commutative, and then we prove that simple rings and primitive rings are prime, with the exception of rings R such that $R^2 = 0$. But for these the conclusion holds trivially. The Brown-Jacobson theory for arbitrary rings then yields a structure theorem for semi-simple weakly standard rings.

Section 3 of the paper is concerned with a proof of the fact that simple flexible rings satisfying (1.2) are either associative or commutative. This generalizes the result for weakly standard rings but appears to be of considerable interest in itself. Various applications of this theorem are mentioned.

The last section contains the example referred to above, as well as examples showing the impossibility of making certain plausible generalizations in our hypotheses.

Throughout the paper we use the letters t, u, v, w, x, y, z to stand for arbitrary elements of the ring under consideration, thus obviating expressions like "for all x and y of the ring."

2. Main results. To facilitate our computations, we begin by defining the following functions:

$$(2.1)\qquad f(w,x,y,z) = (wx,y,z) - (w,xy,z) + (w,x,yz) - w(x,y,z) - (w,x,y)z,$$

$$(2.2)\qquad g(x,y,z) = (xy,z) - x(y,z) - (x,z)y - (x,y,z) - (z,x,y) + (x,z,y).$$

It is well known that each of these functions is identically zero in any ring whatever. We now assume that R is a flexible ring and make

Definition 1. Let

$$S = [s \in R \mid (s,x,y) = 0], \qquad M = [m \in R \mid (x,m,y) = 0].$$

Then we call S the *left nucleus* of R and M the *center nucleus.*

With these definitions, the flexible ring R is weakly standard if and only if commutators are in $S \cap M$. For any $s \in S$, $f(s,x,y,z) = 0$ implies that $(sx,y,z) = s(x,y,z)$ while (1.5) implies that $(x,y,s) = 0$.

Definition 2. A ring R is called *prime* if, whenever I and J are ideals of R such that $IJ = 0$, then either $I = 0$ or $J = 0$.

Our first goal is to prove that a prime ring is weakly standard if and only if it is either associative or commutative. We take a significant step in this direction by letting C be the set of all commutators of a weakly standard ring R and proving

LEMMA 1. *If A is the set of all finite sums of elements of the form $R(C,R)$, then A is an ideal of R.*

Proof. That A is a left ideal is immediately obvious in view of the definition of a weakly standard ring. For any commutator $c \in C$, $g(u,v,c) = 0$ implies that

$$(c,uv) = u(c,v) + (c,u)v. \tag{2.3}$$

Hence consider $x((y,z),u) \cdot v$ and let $c = (y,z)$. Then we get

$$x(c,u) \cdot v = x \cdot (c,u)v = x(c,uv) + xu \cdot (c,v).$$

Thus A is also a right ideal and the lemma is proved.

COROLLARY. *The set B of all finite sums of elements of the form $(C,R)R$ is an ideal of R.*

Henceforth we assume that R is a not associative, weakly standard, prime ring. It follows immediately that R does not have any non-zero absolute zero divisors, since the set of all such absolute zero divisors forms an ideal Z such that $RZ = 0$.

LEMMA 2. $(C,R) = 0$.

Proof. Assume that there exist elements d,e,f in R such that $((d,e),f) \neq 0$ and let $Q = [q \in R \mid q(C,R) = (C,R)q = 0]$. It is easy to verify, using (2.3), that Q is an ideal of R. To prove that $Q \neq 0$ we suppose the contrary and let $c = (x,y)$. From $g(z,c,w) = 0$ we get that $(zc,w) = z(c,w) + (z,w)c$ so that $z(c,w)$ is an element of S. Consequently $(c,w)(z,t,v) = 0$ and also $(z,t,v)(c,w) = 0$. But this implies that all associators are in Q, R is associative, and this is a contradiction. We must therefore conclude that $Q \neq 0$. However, $AQ = QB = 0$ implies that $A = B = 0$, and from this we are led to the fact that $((d,e),f)$ is an absolute zero divisor and hence zero. The now inescapable conclusion is that the lemma is proved.

Henceforth assume that R is not commutative either and select a,b in R such that $d = (a,b) \neq 0$. Let $P = [p \in R \mid pd = dp = 0]$, and observe

that P is an ideal of R. Assume for the moment that $P=0$. From $g(a,b,b)=0$ we infer that $(ab,b)=db$. Thus $0=((ab,b),a)=-d^2$ and this implies that $d=0$, a contradiction. Therefore $P\neq 0$. However, Rd is an ideal of R and $RdP=0$. The hypothesis on R forces the conclusion that $Rd=0$, from which d is an absolute zero divisor and hence zero. This contradiction shows that R must, in fact, be commutative. We have all but proved

THEOREM 1. *Let R be a prime ring. Then R is weakly standard if and only if R is either commutative or associative.*

Proof. It remains only to remark that a commutative ring is flexible with $(R,R)=0$, while an associative ring is automatically weakly standard.

We are now in a position to derive a structure theory for weakly standard rings. If R is simple[2] and $R^2=0$, R is both associative and commutative. If R is simple and $R^2\neq 0$, then R is prime. We consequently have

THEOREM 2. *Let R be a simple ring. Then R is weakly standard if and only if R is either associative or commutative.*

Let us now recall that a ring R is called *primitive* if R contains a regular maximal right ideal E which contains no two-sided ideal of R other than the zero ideal. The following lemma was proved by Kleinfeld [5] using the hypothesis of accessibility. We do not use the hypothesis.

LEMMA 3. *Let R be an arbitrary primitive ring. Then R is a prime ring.*

Proof. Suppose E is a maximal right ideal of R such that $ex-x$ is in E for all x in R and for some e in R. Let I and J be two ideals of R such that $IJ=0$ and assume that $I\neq 0$. Then $I\not\subset E$ so $R=E+I$ and $RJ=EJ\subset E$. Hence $ej\in E$ and thus $-j\in E$, $J\subset E$ and $J=0$.

As an immediate application of the lemma we have

THEOREM 3. *Let R be a primitive ring. Then R is weakly standard if and only if R is either associative or commutative.*

Since it follows from a theorem of Brown (see [4], p. 116) that a semi-simple ring is a subdirect sum of primitive rings, the structure theory for semi-simple weakly standard rings is completely determined by Theorem 3.

---

[2] By a simple ring we mean one which has no proper two-sided ideals.

3. Simple flexible rings. In this section we show that it is possible to improve upon Theorem 2, but in a way that does not seem, at this writing, to carry over to the results of Theorems 1 or 3. The starting point is a remark by Kleinfeld in [5] to the effect that, if D is the set of all finite sums of elements of the form (R,R,R) and $R(R,R,R)$, then D is an ideal of R, where R is any ring whatever.

Assume now that R is flexible and that $(R,R) \subset S$. From $g(x,y,y)=0$ we get $(xy,y)=(x,y)y$ and this identity implies

$$(3.1) \qquad (x,y)(y,u,v)=0.$$

A linearization of (3.1) yields $(x,z)(y,u,v)+(x,y)(z,u,v)=0$ and the substitution $z=s$ gives

$$(3.2) \qquad (x,s)(y,u,v)=0.$$

A similar argument, together with (1.5), implies the analogous

$$(3.3) \qquad (y,u,v)(x,s)=0.$$

At this point we add the requirement that R be a simple ring. If the ideal $D=0$, then R is associative. If $D\neq 0$, the simplicity of R requires that $D=R$. Consequently, any t in R can be expressed as a finite sum of elements of the form (R,R,R) and $R(R,R,R)$. Thus, for any (x,s), (3.3) implies that $t(x,s)=0$. A similar argument, using elements of the form (R,R,R) and $(R,R,R)R$, as well as (3.2), gives $(x,s)t=0$, and therefore (x,s) is an absolute zero divisor. We now have two alternatives: if some $(x,s)\neq 0$, the ideal of absolute zero divisors is all of R and R is both associative and commutative; on the other hand, if $(x,s)=0$, then commutators are automatically in M and Theorem 2 applies. We have proved

THEOREM 4. *Let R be a simple flexible ring. Then commutators are in the left nucleus of R if and only if R is either commutative or associative.*

This result is a considerable generalization of Albert's Theorem 14 ([1], p. 593) that a simple standard algebra is either an associative or a Jordan algebra. But the theorem has other applications. Albert has also proved ([2], p. 519) that a simple, commutative, power-associative algebra, of characteristic prime to 30 and of degree greater than two, is a Jordan algebra. Our Theorem 4 shows that the conclusion of Albert's theorem holds with less restrictive hypotheses. The same remarks apply to Albert's Theorems 1 and 2 in [3].

4. Examples.

Example 1. Let A be an alternative ring of characteristic prime to 3 generated by three elements x, y, z such that $(x, y, z) \neq 0$. Let B be the alternative ring obtained from A by setting all products (in A) containing at least four factors equal to zero, and by preserving all other sums and products. Then $(x, y, z) \neq 0$ in B also. Moreover, B is flexible and trivially weakly standard. However, B does not satisfy (1.1), for otherwise $(x, y, z) = 0$ as a consequence of the alternative law.

This gives an example of a weakly standard ring that is not accessible. Thus our results generalize and subsume those of Kleinfeld in [5].

Example 2. In [1], pp. 588-589, Albert gives an example of a simple flexible algebra over any field F of characteristic not two. A not difficult calculation shows that commutators are not in the left nucleus. This example proves that the hypothesis of Theorem 4 could not be "simple flexible" instead of "simple flexible with commutators in the left nucleus."

Example 3. Let A be an algebra over a field F with basis elements e, u, v, w, z, where the only non-zero products among the basis elements are $e^2 = e$, $eu = ue = v$, $ev = ve = u$, $we = ze = w$. If

$$x = \alpha_1 e + \alpha_2 u + \alpha_3 v + \alpha_4 w + \alpha_5 z, y = \beta_1 e + \beta_2 u + \beta_3 v + \beta_4 w + \beta_5 z,$$
$$\text{and } t = \gamma_1 e + \gamma_2 u + \gamma_3 v + \gamma_4 w + \gamma_5 z$$

are arbitrary elements of A (with the α_i, β_i and γ_i in F), a straightforward calculation shows that

$$(4.1) \quad (x, y, t) = (\alpha_2\beta_1\gamma_1 + \alpha_1\beta_1\gamma_3 - \alpha_3\beta_1\gamma_1 - \alpha_1\beta_1\gamma_2)u + (\alpha_3\beta_1\gamma_1 + \alpha_1\beta_1\gamma_2 - \alpha_2\beta_1\gamma_1 - \alpha_1\beta_1\gamma_3)v.$$

It is easy to see from (4.1) that $(x, y, x) = 0$ so that A is a flexible algebra. Moreover, $\beta_1 = 0$ makes the right hand side of (4.1) vanish. It therefore follows that

$$(4.2) \quad M = [m \in A \mid m = m_2 u + m_3 v + m_4 w + m_5 z].$$

Direct computation shows that

$$(4.3) \quad S = [s \in A \mid s = s_2 u + s_2 v + s_3 w + s_4 z].$$

Now (4.2) and (4.3) together imply that $S \subset M$. Finally

$$(4.4) \quad (x, y) = (\alpha_4\beta_1 + \alpha_5\beta_1 - \alpha_1\beta_4 - \alpha_1\beta_5)w$$

and from this we conclude that commutators are in $S \cap M$. However A is neither associative nor commutative, so that the weakly standard hypothesis alone is not enough for Theorem 2.

Example 4.[3] Let A be an algebra over any field F of characteristic not two and with basis elements e, u, v, where the only non-zero products among basis elements are $e^2 = e$, $eu = ve = v$, $ue = u - v$. Calculations as outlined above show that A is flexible, that $S \subset M$, that commutators are in M, but that commutators are not in S. Hence the definition of weakly standard ring cannot be modified in this direction.

Example 5. Let A be an algebra as above with basis e, u, v, w, where $e^2 = e$, $eu = ue = vw = u$, $wv = -u$, and all other basis products zero. It is easy to see that A is not flexible, but that commutators associate in any of the three places in the associator. Thus the definition of weakly standard ring cannot be modified in this direction either.

THE UNIVERSITY OF OREGON.

REFERENCES.

[1] A. A. Albert, "Power-associative rings," *Transactions of the American Mathematical Society*, vol. 64 (1948), pp. 552-593.

[2] ———, "A theory of power-associative commutative algebras," *ibid.*, vol. 69 (1950), pp. 503-527.

[3] ———, "On commutative power-associative algebras of degree two," *ibid.*, vol. 74 (1953), pp. 323-343.

[4] B. Brown, "An extension of the Jacobson radical," *Proceedings of the American Mathematical Society*, vol. 2 (1951), pp. 114-117.

[5] E. Kleinfeld, "Standard and accessible rings," *Canadian Journal of Mathematics*, vol. 8 (1956), pp. 335-340.

[3] Examples 4 and 5 were constructed by Albert in [1] for a different purpose than we use them here.

DIFFERENTIAL OPERATORS ON A SEMISIMPLE LIE ALGEBRA.*

By HARISH-CHANDRA.

1. Introduction. The object of this paper is to present in as concise and coherent a form as possible, certain results on differential operators which will be needed in two subsequent papers for application to the theory of Fourier transforms on a semisimple Lie algebra $\mathfrak{g}_0$. When $\mathfrak{g}_0$ is compact, this theory is not difficult (see Section 5) although some of the results obtained here (e.g. Thsorems 2 and 3) seem to be new. Therefore the main application of our results will be to the case when $\mathfrak{g}_0$ is noncompact. There it will appear that one can obtain certain formulas of a more or less analytic (as against algebraic) nature, which bear a great resemblance to their counterparts in the compact case (see [4(i)]). However, in view of their non-algebraic character, it would seem rather unlikely that the main burden of their proof could be transferred to the compact case by some formal device such as the "unitarian trick." For instance, let us consider the following example. Let $\mathfrak{g}$ the the Lie algebra of all 2×2 complex matrices of trace zero and G_c its (connected) complex adjoint group. Let $\mathfrak{g}_0$ and $\mathfrak{u}$ be the real subalgebras of $\mathfrak{g}$ consisting of the real and the skew-hermitian matrices respectively and G, U the corresponding real analytic subgroups of G_c. Then $\mathfrak{g}_0 \cap \mathfrak{u} = \mathfrak{h}_0$, where $\mathfrak{h}_0$ is the vector space spanned over the real field R by $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Let f, g be functions of class C^∞ on $\mathfrak{g}_0$ and $\mathfrak{u}$ respectively which vanish outside a compact set. Put

$$\phi_f(t) = t \int_G f(txH)\,dx, \qquad \psi_g(t) = t \int_U g(tuH)\,du \qquad (t \in R)$$

where dx and du are the Haar measures on G and U respectively. It is not difficult to show that ϕ_f is well defined and of class C^∞ for all $t \neq 0$ and one can prove that

$$\operatorname*{Lim}_{t \to 0}((d/dt)\phi_f) = c_1 f(0), \qquad \operatorname*{Lim}_{t \to 0}((d/dt)\psi_g(= c_2 g(0)$$

where c_1, c_2 are nonzero constants independent of f and g. The proof of this formula is quite trivial for g and follows from the fact that

$$\operatorname*{Lim}_{t \to 0} \int_U g(tuH)\,du = g(0),$$

* Received July 30, 1956.

if $\int_U du = 1$. But a similar statement about f is actually false and a much more delicate investigation of ϕ_f is required. Nevertheless the resemblance in the two cases is so striking that one cannot give up the feeling that they both must be governed by some common principle. However a little closer examination reveals important differences. For example if we replace H by $H' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and define

$$\phi_f'(t) = t \int_G f(txH')\,dx,$$

we get $\lim_{t\to 0}((d/dt)\phi_f') = 0$. On the other hand in the compact case H is conjugate to $H'' = \begin{pmatrix} (-1)^{\frac{1}{2}} & 0 \\ 0 & -(-1)^{\frac{1}{2}} \end{pmatrix}$ under U and therefore nothing new is obtained if we replace H by H''. This shows that the situation in the noncompact case is considerably more complicated.

Returning to the general case, let $\mathfrak{g}$ be a semisimple Lie algebra over the complex field C. We shall consider the algebra $\mathfrak{D}(\mathfrak{g})$ of polynomial differential operators on $\mathfrak{g}$ (see Section 2 for the precise definition). Let $\mathfrak{g}_0$ and $\mathfrak{u}$ be two real forms of $\mathfrak{g}$ and suppose $\mathfrak{u}$ is compact. It is clear that the complex group G_c of $\mathfrak{g}$ operates on $\mathfrak{D}(\mathfrak{g})$. Hence we can consider the subalgebra $\mathfrak{J}'$ consisting of those elements in $\mathfrak{D}(\mathfrak{g})$ which are invariant under G_c. The structure of $\mathfrak{J}'$ is, of course, completely determined by $\mathfrak{u}$. On the other hand, elements of $\mathfrak{J}'$ can also be regarded as differential operators on $\mathfrak{g}_0$ and therefore the internal structure of $\mathfrak{J}'$ is reflected in the differential equations on $\mathfrak{g}_0$ and this provides the required link from $\mathfrak{u}$ to $\mathfrak{g}_0$. For instance let $\mathfrak{g}$, $\mathfrak{g}_0$ and $\mathfrak{u}$ be as in the above example. Choose complex coordinates x, y, z in $\mathfrak{g}$ such that the corresponding matrix is given by $\begin{pmatrix} z & x \\ y & -z \end{pmatrix}$. Then if the differential operator.

$$D = \partial^2/\partial z^2 + 4\partial^2/\partial x\partial y$$

is interpreted suitably on $\mathfrak{g}_0$ and $\mathfrak{u}$, one finds that $\phi_{Df} = d^2\phi_f/dt^2$ and $\psi_{Dg} = -d^2\psi_g/dt^2$. This is a special case of a result (Lemma 15) which will be proved in its full generality in another paper (see however [4(h)]).

Theorem 1 (Section 3) is the central result of this paper. In Section 5 we give its applications to the case of a compact semisimple Lie algebra. This discussion also enables us to obtain some algebraic results (e.g. Lemma 18) which are valid in the general case as well. Section 8 is devoted to the detailed study of a special case which will have an important significance for later applications. Theorem 5 contains the main result of this section.

2. Preliminary definitions. Let R and C be the fields of real and complex numbers respectively and E_0 a vector space over R of finite dimension. We consider the symmetric algebra [4(c), p. 191] $S(E)$ over the complexification E of E_0. For any $X \in E_0$ let $\partial(X)$ denote the differential operator on E_0 given by [1]

$$f(Y;\partial(X)) = \{(d/dt)f(Y+tX)\}_{t=0} \qquad (Y \in E_0, f \in C^\infty(E_0), t \in R).$$

Then it is obvious that the mapping $X \to \partial(X)$ can be extended uniquely to an algebraic isomorphism of $S(E)$ (over C) into the algebra of differential operators on E_0. Thus for any $p \in S(E)$, we get a differential operator $\partial(p)$ on E. Now suppose there is given a real nondegenerate symmetric bilinear form $B(X,Y)$ $(X, Y \in E_0)$ on E_0. We extend this form on E by linearity (over C) and then use it to identify E with its dual. In this identification an element $X \in E$ corresponds to the linear function $Y \to B(X,Y)$ $(Y \in E)$ and therefore $S(E)$ can now be regarded as the algebra of all polynomial functions on E. In accordance with this intepretation we shall often refer to elements of $S(E)$ as polynomials on E.

Let $\mathcal{E}$ be the algebra of all differential operators on E_0. Then $\mathcal{E} \supset C^\infty(E_0)$, and therefore $S(E)$ and $\partial(S(E))$ are both subalgebras of $\mathcal{E}$. Let $\mathfrak{D}(E)$ denote the subalgebra of $\mathcal{E}$ generated by $S(E) \cup \partial(S(E))$. The elements of $\mathfrak{D}(E)$ will be called polynomial differential operators on E_0. But, whenever convenient, we can regard an element of $\mathfrak{D}(E)$ also as a *holomorphic* differential operator on the *complex* manifold E. Let H be a group of nonsingular linear mappings of E into itself which preserve B so that $B(xX, xY) = B(X,Y)$ $(X, Y \in E; x \in H)$. Then for any $x \in H$, we shall define an automorphism $d \to d^x$ $(d \in \mathfrak{D}(E))$ of $\mathfrak{D}(E)$. In order to do this we have to define $(d^x f)(X_0)$, where f is a holomorphic function on some neighborhood of X_0 in E. If g is a function defined on a subset V of E, let g^x denote the function on xV given by $g^x(X) = g(x^{-1}X)$ $(X \in xV)$. If V is open and g is holomorphic on V, it is clear that g^x is holomorphic on xV. We now define $(d^x f)(X_0) = (df^{x^{-1}})^x(X_0)$. It is easy to check that the operator d^x so defined, is actually a holomorphic differential operator and $d \to d^x$ is a homomorphism of $\mathfrak{D}(E)$ into the algebra of all holomorphic differential operators on E. Moreover if $p \in S(E)$ it is obvious that p^x is the

[1] M being a differentiable manifold (which need not be connected [4(e), (f)]), we denote by $C^\infty(M)$ the space of all (complex-valued) functions on M of class C^∞ and by $C_c(M)$ the space of continuous functions on M which vanish outside some compact set. If D is a differential operator on M and $f \in C^\infty(M)$, $f(p;D)$ denotes the value of Df at a point p in M (see [4(e), §4]). Moreover $C_c^\infty(M) = C_c(M) \cap C^\infty(M)$.

polynomial function $X \to p(x^{-1}X)$ $(X \in E)$ and similarly $(\partial(X))^x = \partial(xX)$. Therefore $(p\partial(q))^x = p^x\partial(q^x)$ $(p, q \in S(E))$. Since every element in $\mathfrak{D}(E)$ is evidently a sum of elements of the form $p\partial(q)$, it follows that $d^x \in \mathfrak{D}(E)$. Finally, the mapping $d \to d^x$ has the inverse $d \to d^{x^{-1}}$ and so it is an automorphism of $\mathfrak{D}(E)$.

Let $S_r(E)$ $(r \geqq 0)$ denote the subspace of $S(E)$ spanned by elements of the form $X_1X_2 \cdots X_r$ where $X_i \in E$. (In case $r = 0$, $S_r(E) = C$.) As usual a polynomial on E is said to be homogeneous of degree r if it lies in $S_r(E)$. For any two polynomials p, q let $\langle p, q\rangle$ denote the value of $\partial(p)q$ at zero. It is obvious that if p and q are homogeneous, $\langle p, q\rangle = 0$ unless their degrees are equal. Notice that $\langle X, Y\rangle = B(X, Y)$ $(X, Y \in E)$ and it follows from the symmetry of B that $\langle p, q\rangle = \langle q, p\rangle$. In fact, let $(X_1, \cdots, X_n)$ be a base for E such that[2] $B(X_i, X_j) = \delta_{ij}$. Then if $p = \sum_{m_i \geqq 0} a(m_1, \cdots, m_n)X_1^{m_1}X_2^{m_2} \cdots X_n^{m_n}$ $(a(m_1, \cdots, m_n) \in C)$, it is obvious that

$$\langle X_1^{m_1} \cdots X_n^{m_n}, p\rangle = m_1! \cdots m_n!\, a(m_1, \cdots, m_n).$$

Hence

$$\langle q, p\rangle = \sum m_1! \cdots m_n!\, a(m_1, \cdots, m_n) b(m_1, \cdots, m_n)$$

if $q = \sum b(m_1, \cdots, m_n)X_1^{m_1} \cdots X_n^{m_n}$. This also shows that $\langle p, q\rangle = 0$, for all $q \in S(E)$ implies $p = 0$. Moreover $(\partial(p)q)^x = \partial(p^x)q^x$ and therefore $\langle p^x, q^x\rangle = \langle p, q\rangle$ $(x \in H)$.

Let U be a nonempty open subset of E_0. We shall denote by $\mathcal{B}(U)$ the class of all functions $f \in C^\infty(U)$ such that

$$\nu_d(f) = \sup_{X \in U} |f(X; d)| < \infty$$

for every $d \in \mathfrak{D}(E)$. We topologise $\mathcal{B}(U)$ by means of the seminorms ν_d $(d \in \mathfrak{D}(E))$ and in this way $\mathcal{B}(U)$ becomes a locally convex space. If D is a differential operator on U and X a point in U, it is obvious that there exists a unique element $p \in S(E)$ such that $f(X; D) = f(X; \partial(p))$ for every $f \in C^\infty(U)$. *We call $\partial(p)$ the local expression of D at X. It will usually be denoted by D_X.* Let H_0 be a group of nonsingular linear mappings of E_0 into itself. Then for every function f on U and $x \in H_0$, let f^x denote the function on U given by $f^x(X) = f(x^{-1}X)$ $(X \in U)$. Then corresponding to any differential operator D on U, we define a new differential operator D^x on U by $D^xf = (Df^{x^{-1}})^x$ $(f \in C^\infty(U))$. One proves without difficulty that $(D_X)^x = (D^x)_{xX}$ $(X \in U)$. D is said to be invariant under H_0 if $D^x = D$ for all $x \in H_0$.

---

[2] δ_{ij} is the usual Kronecker symbol. It is equal to 1 or 0 according as $i = j$ or not.

Select a fixed square root of -1 in C and denote it by $(-1)^{\frac{1}{2}}$. Also let dX denote the Euclidean measure on E_0 (normalized in some way). Then for any $f \in \mathcal{B}(E_0)$, the Fourier transform $\bar{f}$ of f is defined as follows.

$$\bar{f}(Y) = \int_{E_0} \exp((-1)^{\frac{1}{2}} B(Y,X)) f(X) dX \qquad (Y \in E_0).$$

It is well known [8(I), p. 105] that $\bar{f}$ also lies in $\mathcal{B}(E_0)$ and in fact $f \to \bar{f}$ is a topological mapping of $\mathcal{B}(E_0)$ onto itself. Moreover the measure dX can be so normalized that

$$f(Y) = \int_{E_0} \exp\{-(-1)^{\frac{1}{2}} B(Y,X)\} \bar{f}(X) dX \qquad (Y \in E_0)$$

for every $f \in \mathcal{B}(E_0)$. *This normalization will be called the regular normalization.*

LEMMA 1. *There exist a unique automorphism*[3] $d \to \hat{d}$ *of* $\mathfrak{D}(E)$ *such that* $\hat{X} = -(-1)^{\frac{1}{2}} \partial(X)$ *and* $(\partial(X))^{\wedge} = -(-1)^{\frac{1}{2}} X$ $(X \in E)$. *Moreover* $(df)^{-} = \hat{d}\bar{f}$ *for any* $d \in \mathfrak{D}(E)$ *and* $f \in \mathcal{B}(E_0)$.

Since $\mathfrak{D}(E)$ is generated by $(1, E + \partial(E))$, the uniqueness is obvious. The rest follows immediately from the theory of Fourier transforms [8(I), p. 105].

COROLLARY. *For any d in $\mathfrak{D}(E)$, we can select another element $d' \in \mathfrak{D}(E)$ such that*

$$\int_{E_0} | d\bar{f} | \, dX \leqq \nu_{d'}(f) \qquad (f \in \mathcal{B}(E_0)).$$

Choose a polynomial $p \in S(E)$ such that p is never zero on E_0 and $c = \int_{E_0} | p |^{-1} dX < \infty$. Then if $\phi \in \mathcal{B}(E_0)$,

$$\nu_1(\bar{\phi}) = \sup_{X \in E_0} | \bar{\phi}(X) | \leqq \int_{E_0} | \phi | \, dX \leqq c\nu_1(p\phi).$$

Now it follows from the above lemma that $pd = \hat{d}_1$ for some $d_1 \in \mathfrak{D}(E)$. Hence

$$\int_{E_0} | d\bar{f} | \, dX \leqq c\nu_1(pd\bar{f}) = c\nu_1((d_1 f)^{-}) \leqq c^2 \nu(pd_1 f) \qquad (f \in \mathcal{B}(E_0))$$

and so we can take $d' = c^2 p d_1$.

---

[3] We shall write $d^{\wedge}$, f^{-} respectively instead of $\hat{d}$, $\bar{f}$ whenever it is convenient to do so.

The adjoint of a differential operator D on E_0 is, by definition, the unique differential operator D^* such that

$$\int_{E_0} f(X;D)g(X)\,dX = \int_{E_0} f(X)g(X;D^*)\,dX$$

for all $f, g \in C_c^\infty(E_0)$. The mapping $D \to D^*$ is an anti-automorphism of the algebra of all differential operators on E_0 and $(D^*)^* = D$. In particular if p is a homogeneous element in $S(E)$ of degree m, it is obvious that $p^* = p$ and $(\partial(p))^* = (-1)^m \partial(p)$. This shows that $\mathfrak{D}(E))^* = \mathfrak{D}(E)$ and so we get the following result.

LEMMA 2. *There exists a unique anti-automorphism $d \to d^*$ of $\mathfrak{D}(E)$ such that $p^* = p$ and $(\partial(p))^* = (-1)^m \partial(p)$ for any homogeneous polynomial in $S(E)$ of degree m.*

Again the uniqueness follows from the fact that $\mathfrak{D}(E)$ is generated by $S(E) \cup \partial(S(E))$.

U and H_0 being as before, let τ denote a distribution on U [8(I)] and dX the Euclidean measure on E_0. Then, if F is a measurable and locally summable function on U, we say that[4] $\tau = F$ if

$$\tau(f) = \int_U fF\,dX$$

for every $f \in C_c^\infty(U)$. Let V be a subset of $C_c^\infty(U)$. Then by the C_c^∞-topology on V, we mean the topology induced under the usual topology of $C_c^\infty(U)$ [8(I), p. 67]. Similarly if V' is a subset of $\mathscr{B}(U)$, the $\mathscr{B}$-topology on V' is the one induced on it by $\mathscr{B}(U)$. A distribution τ on E_0 will be called a $\mathscr{B}$-distribution if it is continuous under the $\mathscr{B}$-topology on $C_c^\infty(E_0)$. In case this is so, τ can be extended uniquely to a continuous function on $\mathscr{B}(E_0)$ [8(II, pp. 93-94]. If D is a differential operator and τ a distribution on U, the mapping $f \to \tau(D^*f)$ $(f \in C_c^\infty(U))$, where D^* is the adjoint of D, is also a distribution and it will be denoted by $D\tau$. If τ is continuous with respect to the $\mathscr{B}$-topology, the same holds for $D\tau$ provided $D \in \mathfrak{D}(E)$. τ is said to be invariant under H_0 if $\tau(f^x) = \tau(f)$ for all $f \in C_c^\infty(U)$ and $x \in H_0$. More generally, a $\mathscr{B}$-distribution τ on U is a continuous linear mapping of $\mathscr{B}(U)$ into C. If $D \in \mathfrak{D}(E)$, the mapping $D\tau: f \to \tau(D^*f)$ $(f \in \mathscr{B}(U))$ is also a $\mathscr{B}$-distribution on U.

We now introduce a notation which will be used rather frequently. Let M_1, M_2 be two manifolds and f a function on $M_1 \times M_2$ of class C^∞.

[4] Of course this definition depends on the normalization of dX.

Then if $m_i \in M_i$ and D_i is a differential operator on M_i $(i=1,2)$, we shall denote the value of $(D_1 \times D_2)f$ at (m_1, m_2) by $f(m_1; D_1 : m_2; D_2)$. Moreover D_i will be suppressed in this notation whenever it is 1. For example $f(m_1 : m_2; D_2) = f(m_1; 1 : m_2; D_2)$.

Now suppose F is the complexication in E of a vector subspace F_0 of E. Then $S(F) \subset S(E)$. Let B_F denote the restriction of the bilinear form B on F and suppose B_F is nondegenerate. Then we can identify F with its dual under B_F and thus regard $S(F)$ as the algebra of all polynomial functions on F. For any function f on E_0, let $\bar{f}$ denote its restriction on F_0. Then if $f \in S(E)$, it is clear that $\bar{f}$ is a polynomial function[5] on F_0 and therefore it lies in $S(F)$. Moreover if $f \in S(F)$, $f = \bar{f}$ in $S(E)$. Similarly $\partial(S(F)) \subset \partial(S(E))$ and therefore $\mathfrak{D}(F) \subset \mathfrak{D}(E)$. Elements of $\mathfrak{D}(F)$ can therefore be regarded as differential operators either on F_0 or E_0. But in view of the relation $\overline{df} = d\bar{f}$ $(f \in C^\infty(E_0), d \in \mathfrak{D}(F))$, it is not necessary to distinguish between the two meanings. Also it follows from Lemma 2 that the adjoint operation in $\mathfrak{D}(E)$ coincides on $\mathfrak{D}(F)$ with the corresponding operation in $\mathfrak{D}(F)$. The same obviously holds for the scalar product $\langle p, q \rangle$ $(p, q \in S(F))$.

3. Invariant differential operators. Let $\mathfrak{g}_0$ be a semisimple Lie algebra over R and $\mathfrak{h}_0$ a Cartan subalgebra of $\mathfrak{g}_0$. We denote the corresponding complexifications by $\mathfrak{g}$ and $\mathfrak{h}$ respectively. Then if we take $E_0 = \mathfrak{g}_0$, $F_0 = \mathfrak{h}_0$ and[6] $B(X, Y) = \mathrm{sp}(\mathrm{ad}\, X\, \mathrm{ad}\, Y)$ $(X, Y \in \mathfrak{g}_0)$, all the above conditions are fulfilled. Let G be the (connected) adjoint group of $\mathfrak{g}_0$. Then every $x \in G$ can be regarded as a nonsingular linear transformation of $\mathfrak{g}$ which preserves B and so it defines an automorphism $D \to D^x$ $(D \in \mathfrak{D}(E))$ of $\mathfrak{D}(E)$. We call a function f of $\mathfrak{g}_0$ invariant (under G) if $f^x = f$ $(x \in G)$. Let $I(\mathfrak{g})$ be the set of invariant elements in $S(\mathfrak{g})$. Then, if f is an invariant function in $C^\infty(\mathfrak{g}_0)$ and $p \in I(\mathfrak{g})$, it is obvious that $\partial(p)f$ is also invariant. We would like to express $\overline{\partial(p)f}$ in terms of $\partial(\bar{p})$ and $\bar{f}$ (where the bar denotes restriction on $\mathfrak{h}_0$). Let $\alpha_1, \cdots, \alpha_r$ be all the distinct positive roots of $\mathfrak{g}$ (with respect to $\mathfrak{h}$) under some fixed order (see [4(g), §2]). Then $\pi = \alpha_1\alpha_2 \cdots \alpha_r$ is a polynnomial function on $\mathfrak{h}$. we intend to prove that $\pi\overline{\partial(p)f} = \partial(\bar{p})(\pi\bar{f})$.

First we introduce some notation. Let U be an open subset of $\mathfrak{g}_0$.

---

[5] We agree to identify a polynomial function on E with its restriction on E_0. Similarly for F.

[6] $X \to \mathrm{ad}\, X$ $(X \in \mathfrak{g})$ denotes the adjoint representation of $\mathfrak{g}$.

Select open subsets $\mathfrak{g}_1$, G_1 of $\mathfrak{g}_0$ and G respectively such that $xX \in U$ for $x \in G_1$, $X \in \mathfrak{g}_1$. For any $f \in C^\infty(U)$, consider the function

$$g(x:X) = f(xX) \qquad (x \in G_1, X \in \mathfrak{g}_1)$$

on $G_1 \times \mathfrak{g}_1$. If d and D are differential operators on G_1 and $\mathfrak{g}_1$ respectively, we put $f(x;d:X;D) = g(x;d:X;D)$. (Again we suppress d or D whenever it is 1.) Let $\mathfrak{B}$ be the universal enveloping algebra of $\mathfrak{g}$. Then elements of $\mathfrak{B}$ can be regarded as left-invariant differential operators on G [4(e), §4]. All products of the form $X_1^{m_1} \cdots X_r^{m_r}$ ($X_i \in \mathfrak{g}$) are meant to be in $S(\mathfrak{g})$ unless it is explicitly stated otherwise. Now suppose $Y \in \mathfrak{g}_1$, $p \in S(\mathfrak{g})$ and $f \in C^\infty(U)$. Then

$$f(x:Y;\partial(p)) = f(xY;\partial(p^x)) \qquad (x \in G_1)$$

and therefore if $X \in \mathfrak{g}_0$,

$$f(x;X:Y;\partial(p)) = \{(d/dt)f(x_tY;\partial(p^{x_t}))\}_{t=0} \qquad (t \in R)$$

where $x_t = x \exp tX$. For any $Z \in \mathfrak{g}$, let d_Z denote the derivation of $S(\mathfrak{g})$ which coincides with $\operatorname{ad} Z$ on $\mathfrak{g}$. It is clear that

$$\{(d/dt)f(x_tY;\partial(p^{x_t}))\}_{t=0} = \{(d/dt)f(x_tY;\partial(p^x))\}_{t=0} + \{(d/dt)f(xY;\partial(p^{x_t}))\}_{t=0}$$

and

$$f(x_tY;\partial(p^x)) = f(x:z_tY;\partial(p)),\ f(xY;\partial(p^{x_t})) = f(x:Y;\partial(p^{z_t})),$$

where $z_t = \exp tX$. Hence

$$f(x;X:Y;\partial(p)) = f(x:Y;\partial((d_XY)p + d_Xp)).$$

For any $q \in S(\mathfrak{g})$, let L_q denote the linear mapping $p \to qp$ ($p \in S(\mathfrak{g})$) of $S(\mathfrak{g})$. Then we have the following result.

LEMMA 3. *Let $f \in C^\infty(U)$, $X_1, \cdots, X_r \in \mathfrak{g}$ and $p \in S(\mathfrak{g})$. Moreover let $\cdot$ denote multiplication in $\mathfrak{B}$. Then if $Y \in \mathfrak{g}_1$,*

$$f(x;X_1 \cdot X_2 \cdot \cdots \cdot X_r:Y;\partial(p)) = f(x:Y;\partial(q)) \qquad (x \in G_1),$$

where [7]

$$q = (L_{[X_1,Y]} + d_{X_1})(L_{[X_2,Y]} + d_{X_2}) \cdots (L_{[X_r,Y]} + d_{X_r})p.$$

For $r = 1$ this has been proved above. So now suppose $r > 1$ and use induction. Put

$$q' = (L_{[X_2,Y]} + d_{X_2}) \cdots (L_{[X_r,Y]} + d_{X_r})p.$$

[7] $[X, Y] = d_XY$ ($X, Y \in \mathfrak{g}$) as usual.

Then by induction hypothesis

$$f(x';X_2\cdot\cdots\cdot X_r:Y;\partial(p))=f(x':Y;\partial(q')) \qquad (x'\in G_1).$$

Hence $f(x;X_1\cdot X_2\cdot\cdots\cdot X_r:Y;\partial(p))$

$$=\{(d/dt)f(x\exp tX_1;X_2\cdot\cdots\cdot X_r:Y;\partial(p))\}_{t=0}$$

$$=\{(d/dt)f(x\exp tX_1:Y;\partial(q'))\}_{t=0}$$

$$=f(x;X_1:Y;\partial(q'))=f(x:Y;\partial((L_{[X_1,Y]}+d_{X_1})q')))$$

$=f(x:Y;\partial(q))$. This proves the lemma.

Now consider the tensor product $\mathfrak{B}\times S(\mathfrak{g})$. The above lemma shows[8] that for every $Y\in\mathfrak{g}_0$ there exists a unique bilinear mapping Γ_Y of $\mathfrak{B}\times S(\mathfrak{g})$ into $S(\mathfrak{g})$ such that $\Gamma_Y(1\times p)=p$ and

$$\Gamma_Y(X_1\cdot X_2\cdot\cdots\cdot X_r\times p)=(L_{[X_1,Y]}+d_{X_1})\cdots(L_{[X_r,Y]}+d_{X_r})p$$

$(X_1,\cdots,X_r\in\mathfrak{g};p\in S(\mathfrak{g}))$. For any root α (of $\mathfrak{g}$ with respect to $\mathfrak{h}$), select an element $X_\alpha\neq 0$ in $\mathfrak{g}$ such that $[H,X_\alpha]=\alpha(H)X_\alpha$ for all $H\in\mathfrak{h}$. Put $\mathfrak{s}=\sum_\alpha CX_\alpha$ where α runs over all the roots. Then the symmetric algebra $S(\mathfrak{s})$ over $\mathfrak{s}$ is a subalgebra of $S(\mathfrak{g})$. Let λ denote the canonical mapping [4(c), p. 192] of $S(\mathfrak{g})$ into $\mathfrak{B}$ and put $\mathfrak{S}=\lambda(S(\mathfrak{s}))$.

LEMMA 4. *Let H_0 be an element in $\mathfrak{h}_0$ such that $\pi(H_0)\neq 0$. Then Γ_{H_0} defines a one-one mapping of $\mathfrak{S}\times S(\mathfrak{h})$ onto $S(\mathfrak{g})$.*

Let $S_d(\mathfrak{g})$, $S_d(\mathfrak{s})$ and $S_d(\mathfrak{h})$ denote the spaces of homogeneous elements of degree d in $S(\mathfrak{g})$, $S(\mathfrak{s})$ and $S(\mathfrak{h})$ respectively and put $\mathfrak{S}_d=\lambda(S_d(\mathfrak{s}))$. We shall prove by induction on r that

$$\sum_{d+e\leqq r}\Gamma_{H_0}(\mathfrak{S}_d\times S_e(\mathfrak{h}))=\sum_{s\leqq r}S_s(\mathfrak{g}).$$

This is obvious if $r=0$. So now suppose $r\geqq 1$. It is clear that the left side is contained in the right side. Hence in view of our induction hypothesis it is enough to prove that

$$\sum_{d+e\leqq r}\Gamma_{H_0}(\mathfrak{S}_d\times S_e(\mathfrak{h}))+\mathcal{S}_{r-1}\supset S_r(\mathfrak{g}),$$

where $\mathcal{S}_k=\sum_{s\leqq k}S_s(\mathfrak{g})$. Since $\mathfrak{g}=\mathfrak{h}+\mathfrak{s}$, $S_r(\mathfrak{g})$ is spanned by elements of the form $Z_1Z_2\cdots Z_dH_1H_2\cdots H_e$ $(Z_i\in\mathfrak{S},H_j\in\mathfrak{h})$, where $d+e=r$. Moreover the restriction of $\operatorname{ad}H_0$ on $\mathfrak{s}$ is nonsingular since $\pi(H_0)\neq 0$. Therefore we can select $Y_i\in\mathfrak{s}$ such that $[H_0,Y_i]=-Z_i$ $1\leqq i\leqq d$. Then

[8] The proof of this fact is exactly parallel to that of Lemma 15 of [4(e)].

$$\Gamma_{H_0}(Y_1 \cdot Y_2 \cdot \cdots \cdot Y_d \times H_1 \cdots H_e) = (L_{Z_1} + d_{Y_1}) \cdots (L_{Z_d} + d_{Y_d})(H_1 \cdots H_e)$$
$$\equiv Z_1 Z_2 \cdots Z_d H_1 \cdots H_e \bmod \mathcal{S}_{r-1}.$$

On the other hand $Y_1 \cdot Y_2 \cdot \cdots \cdot Y_d - \lambda(Y_1 Y_2 \cdots Y_d) \in \lambda(\mathcal{S}_{d-1})$ (see [4(a)]) and $\Gamma_{H_0}(\lambda(\mathcal{S}_{d-1}) \times H_1 \cdots H_e) \subset \mathcal{S}_{d+e-1} = \mathcal{S}_{r-1}$. Hence it follows that

$$\Gamma_{H_0}(\lambda(Y_1 \cdots Y_d) \times H_1 H_2 \cdots H_e) - (Z_1 Z_2 \cdots Z_d H_1 \cdots H_e) \in \mathcal{S}_{r-1}$$

and this proves our assertion. Now the spaces $\mathcal{S}_r$ and $\sum_{d+e \leqq r} \mathfrak{S}_d \times S_e(\mathfrak{h})$ have the same dimension from Lemma 12 of [4(c)]. Therefore Γ_{H_0} must be one-one.

Let U and V be two vector spaces over C and suppose the dimension of U is finite. A mapping f of U into V will be called a polynomial mapping if (1) the subspace of V spanned by $f(U)$ is of finite dimension and (2) for every linear function μ on V, $u \to \mu(f(u))$ $(u \in U)$ is a polynomial function on U.

LEMMA 5. *For every $p \in S(\mathfrak{g})$ there exists an integer $r \geqq 0$ and a polynomial mapping γ_p of $\mathfrak{h}$ into $\mathfrak{S} \times S(\mathfrak{h})$ such that $\Gamma_H(\gamma_p(H)) = \pi(H)^r p$ $(H \in \mathfrak{h}_0)$.*

This is proved in substantially the same way as Lemma 16 of [4(e)].

Now put $\mathfrak{S}' = \sum_{d \geqq 1} \mathfrak{S}_d$ and let $\mathfrak{h}_0'$ denote the set of all $H \in \mathfrak{h}_0$ where $\pi(H) \neq 0$. It follows from Lemma 4 that for any $H \in \mathfrak{h}_0'$ and $p \in S(\mathfrak{g})$, there exists a unique element $\beta_H(p) \in S(\mathfrak{h})$ such that $p - \beta_H(p) \in \Gamma_H(\mathfrak{S}' \times S(\mathfrak{h}))$. Hence we can define a mapping $\delta_H'(H \in \mathfrak{h}_0')$ of $\partial(S(\mathfrak{g}))$ into $\partial(S(\mathfrak{h}))$ by $\delta_H'(\partial(p)) = \partial(\beta_H(p))$ $(p \in S(\mathfrak{g}))$. We extend this to a mapping of $\mathfrak{D}(\mathfrak{g})$ into $\partial(S(\mathfrak{g}))$ by setting $\delta_H'(D) = \delta_H'(D_H)$ $(D \in \mathfrak{D}(\mathfrak{g}))$ where D_H is the local expression of D at H. Then it follows from Lemma 5 that there exists an integer $m \geqq 0$ and a polynomial mapping γ of $\mathfrak{h}$ into $\partial(S(\mathfrak{h}))$ such that $\delta_H'(D) = \pi(H)^{-m}\gamma(H)$ $(H \in \mathfrak{h}_0')$. This shows that there exists a differential operator $\delta'(D)$ on $\mathfrak{h}_0'$ whose local expression at any point $H \in \mathfrak{h}_0'$ coincides with $\delta_H'(D)$. The significance of $\delta'(D)$ is given by the following lemma.

LEMMA 6. *Let U be an open neighborhood in $\mathfrak{g}_0$ of a point $H \in \mathfrak{h}_0'$. Suppose f is a function in $C^\infty(U)$ and $f(xX) = f(X)$ whenever (x, X) is sufficiently near $(1, H)$ in $G \times \mathfrak{g}_0$. Then if $\bar{f}$ denotes the restriction of f on $U \cap \mathfrak{h}_0'$, $f(H; D) = \bar{f}(H; \delta'(D))$ for $D \in \mathfrak{D}(\mathfrak{g})$.*

Select $p \in S(\mathfrak{g})$ such that $D_H = \partial(p)$. Then we know that

$$p = \Gamma_H(1 \times \beta_H(p)) + \sum_{i=1}^{r} s_i \times h_i$$

where $s_i \in \mathfrak{S}'$ and $h_i \in S(\mathfrak{h})$. Therefore from Lemma 3,

$$f(x:H;\partial(p)) = f(x:H;\partial(\beta_H(p))) + \sum_{i=1}^{r} f(x;s_i:H;\partial(h_i)),$$

if x lies sufficiently near 1 in G. But it is obvious from our assumption on f that $f(x;b:X) = 0$ $(b \in \mathfrak{B}\mathfrak{g})$ if (x,X) is sufficiently near $(1,H)$ in $G \times \mathfrak{g}_0$. Hence $f(x:H;\partial(p)) = f(x:H;\partial(\beta_H(p)))$. But $\partial(p) = D_H$ and $\partial(\beta_H(p)) = \delta_H'(D_H) = \delta_H'(D)$. Therefore putting $x = 1$, we get $f(H;D) = f(H;\delta_H'(D))$, which is equivalent to the assertion of the lemma.

Let $\mathfrak{J}'$ be the subalgebra consisting of those elements $D \in \mathfrak{D}(\mathfrak{g})$ which are invariant under G.

LEMMA 7. *The mapping $D \rightarrow \delta'(D)$ $(D \in \mathfrak{J}')$ is a homomorphism of $\mathfrak{J}'$ into the algebra of all differential operators on $\mathfrak{h}_0'$.*

Let H_0 be a point in $\mathfrak{h}_0'$ and A the Cartan subgroup of G (see [4(e), §2]) corresponding to $\mathfrak{h}_0$. Let $x \rightarrow x^*$ denote the natural mapping of G on $G^* = G/A$ and put $x^*H = xH$ $(x \in G, H \in \mathfrak{h}_0)$. Select open connected neighborhoods U and V of H_0 and 1 in $\mathfrak{h}_0'$ and G respectively. Let V^* be the image of V in G^*. Then the mapping $\phi: (x^*, H) \rightarrow x^*H$ of $V^* \times U$ into $\mathfrak{g}_0$ is easily seen to be regular (see [4(d), p. 501]). Therefore since the two manifolds $V^* \times U$ and $\mathfrak{g}_0$ have the same dimension, $N = \phi(V^* \times U)$ is an open submanifold of $\mathfrak{g}_0$. Moreover it follows that if V and U are sufficiently small, ϕ is univalent and therefore it defines an analytic isomorphism of $V^* \times U$ onto N. For any $g \in C^\infty(U)$, let f_g denote the function in $C^\infty(N)$ given by $f_g(\phi(x^*, H)) = g(H)$ $(x^* \in V^*, H \in U)$. Then $f_g(xH) = g(H)$ $(x \in V, H \in U)$. Now suppose $D_1, D_2 \in \mathfrak{J}'$ and put $F = D_2 f_g$. Since D_2 is invariant under G, it is clear that Lemma 6 is applicable to F and therefore $F(H;D_1) = \bar{F}(H;\delta'(D_1))$ $(H \in U)$. On the other hand by applying the same lemma to f_g we get

$$\bar{F}(H) = f_g(H;D_2) = g(H;\delta'(D_2)) \qquad (H \in U).$$

Therefore, $f_g(H;D_1D_2) = F(H;D_1) = \bar{F}(H;\delta'(D_1)) = g(H;\delta'(D_1)\delta'(D_2))$. But again from Lemma 6, $f_g(H;D_1D_2) = g(H;\delta'(D_1D_2))$. Therefore, $g(H;\delta'(D_1D_2)) = g(H;\delta'(D_1)\delta'(D_2))$ and this proves that $\delta'(D_1D_2) = \delta'(D_1)\delta'(D_2)$ on U. But since U is a neighborhood of an arbitrary point $H_0 \in \mathfrak{h}_0'$, we conclude that $\delta'(D_1D_2) = \delta'(D_1)\delta'(D_2)$ on $\mathfrak{h}_0'$.

We recall that $I(\mathfrak{g}) = S(\mathfrak{g}) \cap \mathfrak{J}'$. Let $\mathfrak{J}(\mathfrak{g})$ be the subalgebra of $\mathfrak{J}'$ generated by $I(\mathfrak{g}) \cup \partial(I(\mathfrak{g}))$. We shall now determine $\delta'(D)$ for $D \in \mathfrak{J}(\mathfrak{g})$. Obviously, if $p \in I(\mathfrak{g})$, $\delta'(p) = \bar{p}$, where $\bar{p}$ is the restriction of p on $\mathfrak{h}$.

Therefore in view of Lemma 7, it is sufficient to determine $\delta'(D)$ for $D \in \partial(I(\mathfrak{g}))$.

LEMMA 8. *If* $p \in I(\mathfrak{g})$ *then*[9] $\delta'(\partial(p)) = \pi^{-1}\partial(\bar{p}) \circ \pi$.

Define a polynomial function ω on $\mathfrak{g}$ by $\omega(X) = \mathrm{sp}(\mathrm{ad}\,X)^2$ $(X \in \mathfrak{g})$. (We shall call ω the Casimir polynomial of $\mathfrak{g}$.) Then $\omega \in I(\mathfrak{g})$ and we shall first compute $\delta'(\omega)$. Let P be the set of all positive roots. For any $\alpha \in P$, normalize the elements X_α, $X_{-\alpha}$ in such a way that $B(X_\alpha, X_{-\alpha}) = 1$ and put $H_\alpha = [X_\alpha, X_{-\alpha}]$. Then $B(H_\alpha, H) = \alpha(H)$ $(H \in \mathfrak{h})$ and therefore $\alpha = H_\alpha$ under our identification of $\mathfrak{h}$ with its dual. Now consider the polynomial function

$$\xi = \omega - \bar{\omega} - 2 \sum_{\alpha \in P} X_\alpha X_{-\alpha}.$$

If $X = H + \sum_{\alpha \in P} (c_\alpha X_\alpha + c_{-\alpha} X_{-\alpha})$ $(H \in \mathfrak{h}, c_\alpha, c_{-\alpha} \in C)$, it is clear that

$$\omega(X) = \mathrm{sp}(\mathrm{ad}\,X)^2 = \mathrm{sp}(\mathrm{ad}\,H)^2 + 2 \sum_{\alpha \in P} c_{-\alpha} c_\alpha.$$

Therefore, since $B(X, X_\beta) = c_{-\beta}$ for any root β, it follows that $\xi(X) = 0$. Hence $\omega = \bar{\omega} + 2 \sum_{\alpha \in P} X_\alpha X_{-\alpha}$. Now if $H \in \mathfrak{h}_0'$,

$$\Gamma_{H_0}((X_\alpha \cdot X_{-\alpha}) \times 1) = (L_{[X_\alpha, H_0]} + d_{X_\alpha})[X_{-\alpha}, H] = \alpha(H_0) X_\alpha X_{-\alpha} - \alpha(H_0) H_\alpha$$

and $X_\alpha \cdot X_{-\alpha} = \frac{1}{2}(X_\alpha \cdot X_{-\alpha} + X_{-\alpha} \cdot X_\alpha) + \frac{1}{2} H_\alpha$ in $\mathfrak{B}$. Hence

$$\Gamma_{H_0}\Big(\sum_{\alpha \in P} \alpha(H_0)^{-2} (X_\alpha \cdot X_{-\alpha} + X_{-\alpha} \cdot X_\alpha) \times 1 + (1 \times \bar{\omega}) + 2 \sum_{\alpha \in P} \alpha(H_0)^{-1} (1 \times H_\alpha)\Big)$$

$= \bar{\omega} + 2 \sum_{\alpha \in P} X_\alpha X_{-\alpha} = \omega$. This proves that

$$\delta_{H_0}'(\partial(\omega)) = \partial(\bar{\omega}) + 2 \sum_{\alpha \in P} \alpha(H_0)^{-1} \partial(H_\alpha)$$

since $X_\alpha \cdot X_{-\alpha} + X_{-\alpha} \cdot X_\alpha \in \mathfrak{S}'$. On the other hand let us compute $\pi^{-1}\partial(\bar{\omega}) \circ \pi$. For any two differential operators D_1, D_2 put $\{D_1, D_2\} = D_1 \circ D_2 - D_2 \circ D_1$. Then, if $\alpha_1, \cdots, \alpha_r$ are all the distinct positive roots,

$$\{\partial(\bar{\omega}), \pi\} = \sum_{k=1}^{r} \alpha_1 \alpha_2 \cdots \alpha_{k-1} \{\partial(\bar{\omega}), \alpha_k\} \circ (\alpha_{k+1} \cdots \alpha_r).$$

Moreover a simple calculation shows[10] that $\{\partial(\bar{\omega}), \alpha\} = 2\partial(H_\alpha)$. Therefore

$$\partial(\bar{\omega}) \circ \pi = \pi \partial(\bar{\omega}) + 2 \sum_{k=1}^{r} \alpha_1 \alpha_2 \cdots \alpha_{k-1} \partial(H_{\alpha_k}) \circ (\alpha_{k+1} \cdots \alpha_r).$$

---

[9] Whenever it is necessary to avoid confusion, we denote the product of two differential operators D_1, D_2 by $D_1 \circ D_2$.

[10] This is best done by making use of a base $H_1, \cdots, H_l$ for $\mathfrak{h}$ such that $B(H_i, H_j) = \delta_{ij}$ $(1 \leq i, j \leq l)$.

But $\{\partial(H_\alpha), \beta\} = \beta(H_\alpha)$ for any two roots α, β, and so we can conclude that

$$\partial(\bar{\omega}) \circ \pi = \pi\partial(\bar{\omega}) + 2\sum_{k=1}^{r} \alpha_k^{-1}\,\partial(H_{\alpha_k}) + q,$$

where $q \in S(\mathfrak{h})$. Applying both sides of the above equation to the constant function 1, we find that $q = \partial(\bar{\omega})\pi$. But we shall see presently (Lemma 9 and the Corollary to Lemma 10) that $\partial(\bar{\omega})\pi = 0$. Therefore by comparing this with our earlier expression for $\delta_{H_0}{}'(\partial(\omega))$, it follows that $\delta'(\partial(\omega)) = \pi^{-1}\,\partial(\bar{\omega}) \circ \pi$. This proves our assertion in case $p = \omega$.

Now let μ be the derivation of $\mathfrak{D}(\mathfrak{g})$ given by $\mu D = \frac{1}{2}\{\partial(\omega), D\}$ $(D \in \mathfrak{D}(\mathfrak{g}))$. A direct computation shows that $\mu X = \partial(X)$ $(X \in \mathfrak{g})$. We shall now prove by induction on m that $\mu^m(X_1X_2\cdots X_m) = m!\,\partial(X_1X_2\cdots X_m)$ for $X_1,\cdots,X_m \in \mathfrak{g}$. Since $\mu^2 X = \mu\partial(X) = 0$ $(X \in \mathfrak{g})$, it follows from the Leibnitz rule for derivations that

$$\mu^m(X_1X_2\cdots X_m) = (\mu^m(X_1\cdots X_m)) \circ X_m + m\mu^{m-1}(X_1\cdots X_{m-1}) \circ \mu X_m.$$

But $\mu^{m-1}(X_1\cdots X_{m-1}) = (m-1)!\,\partial(X_1X_2\cdots X_{m-1})$ by induction hypothesis. Therefore $\mu^m(X_1\cdots X_{m-1}) = 0$ and

$$\mu^m(X_1X_2\cdots X_m) = m!\,\partial(X_1\cdots X_{m-1}) \circ \mu X_m = m!\,\partial(X_1\cdots X_{m-1}X_m).$$

This shows that if q is a homogeneous element in $S(\mathfrak{g})$ of degree m, then $\mu^m q = m!\,\partial(q)$.

On the other hand let us put $\bar{\mu}\xi = \frac{1}{2}\{\delta'(\omega), \xi\}$ for any differential operator ξ on $\mathfrak{h}_0{}'$. Then $\bar{\mu}$ is a derivation of the algebra of differential operators on $\mathfrak{h}_0{}'$ and it follows from Lemma 7 that $\delta'(\mu D) = \bar{\mu}\delta'(D)$ for $D \in \mathfrak{J}'$. Let p be a homogeneous element in $I(\mathfrak{g})$ of degree m. Since $\mathfrak{J}'$ is obviously stable under μ, we conclude that

$$m!\,\delta'(\partial(p)) = \delta'(\mu^m p) = \bar{\mu}^m\delta'(p) = \bar{\mu}^m\bar{p}.$$

Now let $\mathfrak{A}$ be an associative algebra and for any $a \in \mathfrak{A}$, let d_a denote the derivation of $\mathfrak{A}$ defined by $d_a b = \frac{1}{2}(ab - ba)$ $(b \in \mathfrak{A})$. Then one proves easily by induction on k that

$$d_a{}^k b = 2^{-k}\sum_{0 \leqq r \leqq k} C_r{}^k(-1)^r a^{k-r}ba^r \qquad (k \geqq 0).$$

We now suppose that $\mathfrak{A}$ has a unit element, c is an element in $\mathfrak{A}$ with an inverse c^{-1} and $a' = c^{-1}ac$. Then if $b \in \mathfrak{A}$ and it commutes with c, it is clear that

$$d_{a'}{}^k b = c^{-1}(d_a{}^k b)c \qquad (k \geqq 0).$$

Let us now take $\mathfrak{A}$ to be the algebra of all differential operators on $\mathfrak{h}_0'$. Then if $a = \partial(\bar{\varpi})$, $b = \bar{p}$ and $c = \pi$, all the above conditions are fulfilled and $a' = \pi^{-1}\partial(\bar{\varpi}) \circ \pi = \delta'(\omega)$ as we have seen above. Moreover if q is any homogeneous element in $S(\mathfrak{h})$ of degree k, we prove in the same way as above that $d_a{}^k q = k!\,\partial(q)$. Therefore

$$\mu^m \bar{p} = d_{a'}{}^m \bar{p} = \pi^{-1}(d_a{}^m \bar{p}) \circ \pi = m!\,\pi^{-1}\,\partial(\bar{p}) \circ \pi$$

and this proves that $\delta'(\partial(p)) = \pi^{-1}\,\partial(\bar{p}) \circ \pi$ for any homogeneous element $p \in I(\mathfrak{g})$. But it is obvious that $I(\mathfrak{g}) = \sum_{m \geqq 0} I(\mathfrak{g}) \cap S_m(\mathfrak{g})$ and so the assertion of the lemma follows.

Let W denote the Weyl group of $\mathfrak{g}$ with respect to $\mathfrak{h}$ (see [4(b), p. 29]). Then W is a group of nonsingular linear mappings of $\mathfrak{h}$ and therefore (see Section 2) it operates on $\mathfrak{D}(\mathfrak{h})$. Let $\mathfrak{J}(\mathfrak{h})$ denote the subalgebra of those elements in $\mathfrak{D}(\mathfrak{h})$ which are invariant under W.

THEOREM 1. *There exists a unique homomorphism δ of $\mathfrak{J}(\mathfrak{g})$ into $\mathfrak{J}(\mathfrak{h})$ such that $\delta(p) = p$ and $\delta(\partial(p)) = \partial(\bar{p})$ $(p \in I(\mathfrak{g}))$. Moreover $\delta'(D) = \pi^{-1}\delta(D) \circ \pi$ on $\mathfrak{h}_0'$ for any $D \in \mathfrak{J}(\mathfrak{g})$.*

Since $\mathfrak{J}(\mathfrak{g})$ is generated by $I(\mathfrak{g}) \cup \partial(I(\mathfrak{g}))$, the uniqueness of δ is obvious. Let $\mathfrak{H}'$ denote the algebra of all differential operators on $\mathfrak{h}_0'$. It is clear that we can regard $\mathfrak{D}(\mathfrak{h})$ as a subalgebra of $\mathfrak{H}'$. Put $\delta(D) = \pi\delta'(D) \circ \pi^{-1}$. Then it follows from Lemma 7, that δ is a homomorphism of $\mathfrak{J}(\mathfrak{g})$ into $\mathfrak{H}'$. Moreover $\delta(p) = \bar{p}$, $\delta(\partial(p)) = \partial(\bar{p})$ $(p \in I(\mathfrak{g}))$ from Lemma 8 and $\bar{p}$ is invariant under W (see Lemma 9 below). Therefore it is obvious that δ maps $\mathfrak{J}(\mathfrak{g})$ into $\mathfrak{J}(\mathfrak{h})$ and so the theorem is proved.

4. Invariants of the Weyl group. An element $q \in S(\mathfrak{h})$ is said to be invariant (under W) if $q^s = q$ for all $s \in W$. Let $I(\mathfrak{g})$ be the subalgebra of $S(\mathfrak{h})$ consisting of all invariants. The following result is due to Chevalley (see [1, exposé 19, p. 10]).

LEMMA 9 (Chevalley). *If $p \in I(\mathfrak{g})$, then $\bar{p} \in I(\mathfrak{h})$, and $p \to \bar{p}$ is an isomorphism of $I(\mathfrak{g})$ onto $I(\mathfrak{h})$.*

For any root α let s_α denote the Weyl reflexion corresponding to α. An element $q \in S(\mathfrak{h})$ will be called skew (or skew-invariant) if $q^{s_\alpha} = -q$ for every root α. It is known (see Weyl [9]) that π is skew.

LEMMA 10. *If q is a skew-invariant in $S(\mathfrak{h})$, then $q = \pi q_0$ for some $q_0 \in I(\mathfrak{h})$.*

For any root α, let σ_α denote the hyperplane in $\mathfrak{h}$ given by the equation $\alpha = 0$. Then if $p \in S(\mathfrak{h})$, it follows from the definition of s_α that $p^{s_\alpha} - p$ vanishes everywhere on σ_α. Therefore $p^{s_\alpha} - p$ is divisible by α in the polynomial ring $S(\mathfrak{h})$. This shows that $q = -\frac{1}{2}(q^{s_\alpha} - q)$ is divisible by α. Now the hyperplanes σ_α corresponding to distinct positive roots α are distinct. Therefore since $S(\mathfrak{h})$ is a unique factorization domain, q is divisible by $\prod_{\alpha \in P} \alpha = \pi$. This means that $q = \pi q_0$, where $q_0 \in S(\mathfrak{h})$. But since both π and q are skew, it follows that $q_0^{s_\alpha} = q_0$ $(\alpha \in P)$. Therefore since W is generated by the reflexions s_α $(\alpha \in P)$, we conclude that $q_0 \in I(\mathfrak{h})$.

COROLLARY. *If q is a homogeneous element in $I(\mathfrak{h})$ of positive degree, then $\partial(q)\pi = 0$.*

Let r be the degree of π. Then it is obvious that $\partial(q)\pi$ is homogeneous and its degree is lower than r. On the other hand, since $q \in I(\mathfrak{h})$, it is clear that $\partial(q)\pi$ is a skew-invariant. Therefore in view of the above lemma, we conclude that $\partial(q)\pi = 0$.

Put $S = S(\mathfrak{h})$ and $J = I(\mathfrak{h})$ and let J_+ be the ideal in J spanned by all homogeneous elements of J of positive degree. Since W is a finite group generated by reflexions. it follows from a result of Chevalley [2] that the dimension of the vector space S/J_+S is equal to the order w of W. Moreover if Q_S and Q_J are the quotient fields of S and J respectively, then $[Q_S : Q_J] = w$ where $[Q_S : Q_J]$ denotes, as usual, the degree of the field-extension Q_S/Q_J. It is obvious that if an element of S lies in J, the same holds for all its homogeneous components. Hence we can select homogeneous elements $v_1, \cdots, v_w \in S$ such that $S = V + J_+S$, where V is the linear space spanned over C by $(v_1, \cdots, v_w)$.

LEMMA 11. *Every element v of $S(\mathfrak{h})$ can be written exactly in one way in the form $v = u_1v_1 + \cdots + u_wv_w$, where $u_i \in I(\mathfrak{h})$ $(1 \leqq i \leqq w)$.*

It follows easily by induction on m that $S = JV + J_+^mS$ $(m \geqq 1)$. Let v be any homogeneous element in S of degree d and let d_i be the degree of v_i. Choose $m > d$ and select elements $u_i', \cdots, u_w' \in J$ such that $v - (u_1'v_1 + \cdots + u_w'v_w) \in J_+^mS$. Let u_i denote the homogeneous component of u_i' of degree $d - d_i$. Then, by considering the homogeneous component of of degree d in the above relation, it is clear that $v - (u_1v_1 + \cdots + u_wv_w) = 0$. This proves that $S = Jv_1 + \cdots + Jv_w$ and now it follows easily that $Q_S = Q_JS = \sum_{i=1}^{w} Q_Jv_i$. However $[Q_S : Q_J] = w$ and so $v_1, \cdots, v_w$ must be

linearly independent over Q_J. This proves that an element $v \in S$ can be written in exactly one way in the form $v = u_1 v_1 + \cdots + u_w v_w$ $(u_i \in J)$.

We shall now make use of the above lemma to obtain some results on the solutions of a certain system of differential equations which will be important for our applications.

LEMMA 12. *Let τ be a distribution on an open subset U of $\mathfrak{h}_0$. Suppose for each $q \in I(\mathfrak{h})$, there exists a complex number c_q such that $\partial(q)\tau = c_q\tau$. Then τ coincides with an analytic function on U.*

Let $H_1, \cdots, H_l$ be a base for $\mathfrak{h}_0$ over R. Put $\Omega = H_1^2 + H_2^2 + \cdots + H_l^2 \in S(\mathfrak{h})$ and consider the polynomial

$$\prod_{s \in W} (\zeta - \Omega^s) = \zeta^w + q_1 \zeta^{w-1} + \cdots + q_w$$

in the indeterminants ζ with coefficients $q_i \in I(\mathfrak{h})$. Then

$$\Omega^w + \Omega^{w-1} q_1 + \cdots + q_w = \prod_{s \in W} (\Omega - \Omega^s) = 0$$

and therefore $\{\partial(\Omega)^w + c_1 \partial(\Omega)^{w-1} + \cdots + c_w\}\tau = 0$, where $c_i = c_{q_i}$ $(1 \leqq i \leqq w)$. However the above differential equation is obviously of the elliptic type (see [3] for the definition of ellipticity). Therefore (see Schwartz [8(I), p. 136] and John [5]), τ is an analytic function on U.

LEMMA 13. *Define $(v_1, \cdots, v_w)$ as in Lemma 11 and let ϕ be an analytic function on a nonempty open connected subset U of $\mathfrak{h}_0$. Suppose ϕ is an eigenfunction of $\partial(u)$ for every $u \in I(\mathfrak{h})$. Then if $\partial(v_i)\phi$ $(1 \leqq i \leqq w)$ all vanish simultaneously at some point of U, ϕ must be identically zero.*

Suppose $\phi(H_0; \partial(v_i)) = 0$ $(1 \leqq i \leqq w)$ for some $H_0 \in U$. For any $v \in S(\mathfrak{h})$, we can select $u_1, \cdots, u_w \in I(\mathfrak{h})$ such that $v = \sum_{i=1}^{w} u_i v_i$ (Lemma 11). But then $\partial(u_i)\phi = c_i \phi$ $(c_i \in C)$ and therefore

$$\phi(H_0; \partial(v)) = \sum_{i=1}^{w} c_i \phi(H_0; \partial(v_i)) = 0.$$

This shows that all derivatives of ϕ vanish at H_0 and so ϕ, being an analytic function, must be identically zero.

COROLLARY. *Suppose H' is a point in $\mathfrak{h}$ such that $\pi(H') \neq 0$ and ϕ an analytic function on U satisfying the system of differential equations*

$$\partial(q)\phi = q(H')\phi \qquad (q \in I(\mathfrak{h})).$$

Then there exist constants c_s $(s \in W)$ such that

$$\phi(H) = \sum_{s \in W} c_s \exp B(H, sH') \qquad (H \in U).$$

Moreover they are uniquely determined.

It follows from Lemma 4 of [4(e)] that the w points sH' $(s \in W)$ are all distinct. Put $\phi_s(H) = \exp B(H, sH')$ $(H \in U)$. Then ϕ_s $(s \in W)$ are linearly independent analytic functions on U (see Lemma 41 of [4(b)]). Moreover since $\partial(H)\phi_s = B(H, sH')\phi_s$ $(H \in \mathfrak{h})$, it is clear that $\partial(q)\phi_s = q(H')\phi_s$ for $q \in I(\mathfrak{h})$. Therefore ϕ_s is a solution of our system of differential equations. Let E be the vector space (over C) consisting of all analytic solutions of this system. It is obviously enough to prove that ϕ_s $(s \in W)$ form a base for E or, what is equivalent, that $\dim E \leqq w$. Choose a point $H_0 \in U$. Assuming that $\dim E > w$, we can select $\phi \neq 0$ in E satisfying the w linear conditions $\phi(H_0; \partial(v_i)) = 0$ $1 \leqq i \leqq w$. But we know from Lemma 13 that this is impossible.

The following lemma will be required in another paper.

LEMMA 14. *Suppose ϕ is an analytic function on U such that $\partial(q)\phi = 0$ for all homogeneous elements $q \in I(\mathfrak{h})$ of positive degree. Then there exists a polynomial function $p \in S(\mathfrak{h})$ such that $\phi = p$ on U.*

For any $H \in \mathfrak{h}$, consider the polynomial

$$\prod_{s \in W} (\zeta - sH) = \zeta^w + q_1\zeta^{w-1} + \cdots + q_w$$

in the indeterminants ζ with coefficients $q_i \in I(\mathfrak{h})$. Then $H^w + H^{w-1}q_1 + \cdots + q_w = 0$; and therefore $\partial(H^w + H^{w-1}q_1 + \cdots + q_w)\phi = 0$. But since q_i are all homogeneous and of positive degree, $\partial(q_i)\phi = 0$ $(1 \leqq i \leqq w)$ and therefore $\partial(H^w)\phi = 0$. Hence if $H_1, \cdots, H_l$ is a base for $\mathfrak{h}_0$ over R, $\partial(H_i^w)\phi = 0$ $1 \leqq i \leqq l$. Obviously, this implies that ϕ is a polynomial of degree $\leqq lw$.

5. Applications to the compact case. In this section we shall assume that G is compact. Let dx denote the normalized Haar measure of G, so that $\int_G dx = 1$. For any $f \in C^\infty(\mathfrak{g}_0)$, let ϕ_f denote the function on $\mathfrak{h}_0$ given by

$$\phi_f(H) = \pi(H) \int_G f(xH)\,dx \qquad (H \in \mathfrak{h}_0).$$

It is obvious that $\phi_f \in C^\infty(\mathfrak{h}_0)$. Define δ as in Theorem 1.

LEMMA 15. *$\phi_{\xi f} = \delta(\xi)\phi_f$ for $\xi \in \mathfrak{J}(\mathfrak{g})$ and $f \in C^\infty(\mathfrak{g}_0)$.*

We use the notation of Section 3. It follows from Lemmas 3 and 5 that

we can select elements $s_i \in \mathfrak{S}'$, $h_i \in S(\mathfrak{h})$ and analytic functions a_i $(1 \leqq i \leqq m)$ on $\mathfrak{h}_0{}'$ such that

$$f(xH;\xi) = f(x:H;\delta'(\xi)) + \sum_{i=1}^{m} a_i(H) f(x;s_i:H;\partial(h_i))$$

for $H \in \mathfrak{h}_0{}'$. But it is obvious that $\int_G f(x;b:H)dx = 0$ $(H \in \mathfrak{h}_0)$ for $b \in \mathfrak{B}\mathfrak{g}$. Hence it follows from Theorem 1 that

$$\phi_{\xi f}(H) = \pi(H) \int_G f(x:H;\delta'(\xi))dx = \phi_f(H;\delta(\xi)) \qquad (H \in \mathfrak{h}_0{}').$$

However, $\phi_{\xi f}$ and $\delta(\xi)\phi_f$ are both in $C^\infty(\mathfrak{h}_0)$ and $\mathfrak{h}_0{}'$ is dense in $\mathfrak{h}_0$. Therefore $\phi_{\xi f} = \delta(\xi)\phi_f$.

LEMMA 16. *$\phi_f(0;\delta(\pi)) = \langle\pi,\pi\rangle f(0)$ for all $f \in C^\infty(\mathfrak{g}_0)$.*

Put $g(H) = \int f(xH)dx$ $(H \in \mathfrak{h}_0)$. Since π is a homogeneous polynomial, it is obvious that the local expression of $\partial(\pi) \circ \pi$ at the origin is exactly $\langle\pi,\pi\rangle$. Hence the value of $\partial(\pi)\phi_f$ at zero is $\langle\pi,\pi\rangle g(0) = \langle\pi,\pi\rangle f(0)$.

As usual, we define $\epsilon(s) = 1$ or -1 according as $\pi^s = \pi$ or $-\pi$ $(s \in W)$.

THEOREM 2.

$$\pi(H)\pi(H') \int_G \exp B(xH,H')dx = w^{-1}\langle\pi,\pi\rangle \sum_{s \in W} \epsilon(s) \exp B(sH,H')$$

for all $H, H' \in \mathfrak{h}$.

Select an element $H' \in \mathfrak{h}$ such that $\pi(H') \neq 0$, and put $f(X) = \exp B(X,H')$ $(X \in \mathfrak{g}_0)$. Then

$$\phi_f(H) = \pi(H) \int_G \exp B(xH,H')dx$$

and therefore, from Theorem 1 and Lemma 15, $\phi_{\partial(p)f} = \partial(\bar{p})\phi_f$ $(p \in I(\mathfrak{g}))$. But it is clear that $\partial(Y)f = B(Y,H')f$ $(Y \in \mathfrak{g})$, and so $\partial(q) = q(H')f$ for $q \in S(\mathfrak{g})$. Hence $\partial(\bar{p})\phi_f = p(H')\phi_f$ $(p \in I(\mathfrak{g}))$. But in view of Lemma 9, this implies that $\partial(q)\phi_f = q(H')\phi_f$ for all $q \in I(\mathfrak{h})$, and we conclude from the Corollary to Lemma 13 that

$$\phi_f(H) = \sum_{s \in W} c_s \exp B(sH,H') \qquad (H \in \mathfrak{h}_0),$$

where c_s $(s \in W)$ are constants. On the other hand, since G is compact, we can select, for each $s \in W$, an element $x_s \in G$ such that $x_sH = sH$ $(H \in \mathfrak{h}_0)$.

Therefore it is obvious that s maps $\mathfrak{h}_0$ into itself and $\phi_f(sH)=\epsilon(s)\phi_f(H)$, and so

$$\phi_f(H)=w^{-1}\sum_{s\in W}\epsilon(s)\phi_f(sH)=w^{-1}c\sum_{s\in W}\epsilon(s)\exp B(sH,H') \qquad (H\in\mathfrak{h}_0),$$

where $c=\sum_{s\in W}\epsilon(s)c_s$. On the other hand, $\phi_f(0;\partial(\pi))=\langle\pi,\pi\rangle f(0)=\langle\pi,\pi\rangle$ from Lemma 16. Put $\psi_s(H)=\exp B(sH,H')$ $(H\in\mathfrak{h}_0)$. Then $\partial(q)\psi_s=q(s^{-1}H')\psi_s$ $(q\in S(\mathfrak{h}))$, and therefore $\partial(\pi)\psi_s=\epsilon(s)\pi(H')\psi_s$. Hence

$$\langle\pi,\pi\rangle=\phi_f(0;\partial(\pi))=w^{-1}c\pi(H')w=c\pi(H'),$$

and so $c=\langle\pi,\pi\rangle/\pi(H')$. This proves that

$$\pi(H)\pi(H')\int_G\exp B(x,H,H')dx=w^{-1}\langle\pi,\pi\rangle\sum_{s\in W}\epsilon(s)\exp B(sH,H')$$

for $H\in\mathfrak{h}_0$ and $H'\in\mathfrak{h}$ provided $\pi(H')\neq0$. But since both sides can obviously be considered as holomorphic functions on $\mathfrak{h}\times\mathfrak{h}$, it follows that they must be equal for all $H,H'\in\mathfrak{h}$.

Let dX and dH denote the Euclidean measures on $\mathfrak{g}_0$ and $\mathfrak{h}_0$, respectively. We may assume (see Lemma 9 of [4(d)]) that they are so normalized that

$$\int_{\mathfrak{g}_0}f(X)dX=\int_{\mathfrak{h}_0}|\pi(H)|^2dH\int_Gf(xH)dx \qquad (f\in C_c(\mathfrak{g}))$$

For any $f\in\mathcal{C}(\mathfrak{g}_0)$ and $g\in\mathcal{C}(\mathfrak{h}_0)$, let $\tilde{f}$ and $\tilde{g}$ denote the corresponding Fourier transforms, so that

$$\tilde{f}(Y)=\int_{\mathfrak{g}_0}\exp\{(-1)^{\frac{1}{2}}B(Y,X)\}f(X)dX,$$
$$\tilde{g}(H')=\int_{\mathfrak{h}_0}\exp\{(-1)^{\frac{1}{2}}B(H',H)\}g(H)dH$$

$(Y\in\mathfrak{g}_0,H'\in\mathfrak{h}_0)$. Then we have the following result.

THEOREM 3. *If $f\in\mathcal{C}(\mathfrak{g}_0)$, the corresponding function ϕ_f lies in $\mathcal{C}(\mathfrak{h}_0)$ and $f\to\phi_f$ is a continuous mapping of $\mathcal{C}(\mathfrak{g}_0)$ into $\mathcal{C}(\mathfrak{h}_0)$. Moreover*[3] *$\phi_{\tilde{f}}=(-1)^r\langle\pi,\pi\rangle(\phi_f)^{\sim}$, where r is the number of positive roots.*

It is seen without difficulty that for any $D\in\mathfrak{D}(\mathfrak{g})$, we can find a finite number of elements $D_1,\cdots,D_m\in\mathfrak{D}(\mathfrak{g})$ and analytic functions $a_1,\cdots,a_m$ on G such that $D^x=a_1(x)D_1+\cdots+a_m(x)D_m$ $(x\in G)$. Now suppose $f\in\mathcal{C}(\mathfrak{g}_0)$ and $d\in\mathfrak{D}(\mathfrak{h})$. Then it is clear that

$$\phi_f(H;d)=\int_Gf(xH;D^x)dx \qquad (H\in\mathfrak{h}_0)$$

where $D = d \circ \pi$. Since G is compact, we can select a positive number c such that $|a_i(x)| \leqq c$ $(1 \leqq i \leqq m, x \in G)$. Hence

$$|\phi_f(H;d)| \leqq \sum_{i=1}^{m} c \sup_{X \in \mathfrak{g}_0} |f(X;D_i)|,$$

and this proves that $\phi_f \in \mathcal{C}(\mathfrak{h}_0)$ and the mapping $f \to \phi_f$ of $\mathcal{C}(\mathfrak{g}_0)$ into $\mathcal{C}(\mathfrak{h}_0)$ is continuous.

Put $\eta(X:Y) = \exp\{(-1)^{\frac{1}{2}} B(X,Y)\}$ $(X, Y \in \mathfrak{g}_0)$. Then if $f \in \mathcal{C}(\mathfrak{g}_0)$,

$$\phi_{\hat{f}}(H) = \pi(H) \int_G \hat{f}(xH)dx = \pi(H) \int_G dx \int_{\mathfrak{g}_0} \eta(xH:Y)f(Y)dY \quad (H \in \mathfrak{h}_0).$$

But

$$\int_{\mathfrak{g}_0} \eta(xH:Y)f(Y)dY = \int_{G\times\mathfrak{h}_0} \eta(xH:yH') \,|\pi(H')|^2 f(yH')dy\, dH'$$
$$= (-1)^r \int_{G\times\mathfrak{h}_0} \eta(xH:yH')\pi(H')^2 f(yH')dy\, dH'$$

since every root takes only pure imaginary values on $\mathfrak{h}_0$. Therefore we conclude from Theorem 2 that

$$\phi_{\hat{f}}(H) = w^{-1}\langle\pi,\pi\rangle(-1)^r \sum_{s \in W} \epsilon(s) \int_{G\times\mathfrak{h}_0} \pi(H')\eta(sH:H')f(yH')dy\, dH'$$
$$= (-1)^r w^{-1}\langle\pi,\pi\rangle \sum_{s \in W} \epsilon(s) \int_{\mathfrak{h}_0} \eta(sH:H')\phi_f(H')dH'.$$

But we have seen that $\phi_f(sH') = \epsilon(s)\phi_f(H')$ $(s \in W)$. Hence

$$\int_{\mathfrak{h}_0} \eta(sH:H')\phi_f(H')dH' = \int_{\mathfrak{h}_0} \eta(H:H')\phi_f(sH')dH'$$
$$= \epsilon(s) \int_{\mathfrak{h}_0} \eta(H:H')\phi_f(H')dH'.$$

This proves that $\phi_{\hat{f}}(H) = (-1)^r\langle\pi,\pi\rangle \int \eta(H:H')\phi_f(H')dH'$ $(H \in \mathfrak{h}_0)$, and therefore $\phi_{\hat{f}} = (-1)^r\langle\pi,\pi\rangle(\phi_f)^{\hat{}}$.

In another paper we shall obtain a suitable analogue of the above theorem for the case when G is not compact.

Let $J(\mathfrak{g}_0)$ and $J(\mathfrak{h}_0)$ denote the sets of all functions in $\mathcal{C}(\mathfrak{g}_0)$ and $\mathcal{C}(\mathfrak{h}_0)$ which are invariant under G and W respectively. For any function f on $\mathfrak{g}_0$, let $\bar{f}$ denote its restriction on $\mathfrak{h}_0$.

THEOREM 4. *If $f \in J(\mathfrak{g}_0)$, then $\bar{f} \in J(\mathfrak{h}_0)$ and $f \to \bar{f}$ is a topological mapping of $J(\mathfrak{g}_0)$ onto $J(\mathfrak{h}_0)$.*

Put $\eta'(X:Y)=\exp\{-(-1)^{\frac{1}{2}}B(X,Y)\}$ $(X,Y\in\mathfrak{g}_0)$. Then if $p\in S(\mathfrak{g})$, it is clear that $\eta'(X;\partial(p):Y)=\hat{p}(Y)\eta'(X:Y)$ where $\hat{p}$ is the polynomial function $Z\to p(-(-1)^{\frac{1}{2}}Z)$ on $\mathfrak{g}$. Now we assume that the normalization of the Euclidean measure dH on $\mathfrak{h}_0$ is regular and put

$$\psi_g(X)=\int_{\mathfrak{h}_0}\xi(X:H)\pi(H)\bar{g}(H;\partial(\pi))dH \qquad (g\in J(\mathfrak{h}_0), X\in\mathfrak{g}_0),$$

where $\xi(X:Y)=\int_G\eta'(xX:Y)dx$ $(X,Y\in\mathfrak{g}_0)$. Then it follows from Theorem 2 that if $H'\in\mathfrak{h}_0$,

$$\pi(H')\psi_g(H')=c\int_{\mathfrak{h}_0}\sum_{s\in W}\epsilon(s)\eta'(H:sH')\bar{g}(H;\partial(\pi))dH,$$

where $c=w^{-1}\langle\pi,\pi\rangle$. Now it is clear that[11]

$$\int_{\mathfrak{h}_0}\eta'(H:sH')\bar{g}(H;\partial(\pi))dH=(-1)^r\int_{\mathfrak{h}_0}\eta'(H;\partial(\pi):sH')\bar{g}(H)dH$$

$$=(-1)^r\hat{\pi}(sH')\int\eta'(H:sH')\bar{g}(H)dH=(-1)^{r/2}\epsilon(s)\pi(H')g(sH')$$

$(s\in W)$. Therefore, since g is invariant under W, we get

$$\pi(H')\psi_g(H')=(-1)^{r/2}wc\pi(H')g(H') \qquad (H'\in\mathfrak{h}_0).$$

But as $\bar{\psi}_g$ and g are both of class C^∞, this implies that $\bar{\psi}_g=c'g$, where $c'=(-1)^{r/2}\langle\pi,\pi\rangle$. It is obvious from its definition that $\psi_g\in C^\infty(\mathfrak{g}_0)$ and it is invariant under G. Moreover, since $\mathfrak{g}_0=\bigcup_{x\in G}x\mathfrak{h}_0$, it is obvious that ψ_g is the only invariant function on $\mathfrak{g}_0$ which coincides with $c'g$ on $\mathfrak{h}$. Therefore $q\psi_g=\psi_{\bar{q}g}$ if $q\in I(\mathfrak{g})$.

Put

$$\nu_D(F)=\sup_{X\in\mathfrak{g}_0}|F(X;D)|, \qquad \sigma_d(\phi)=\sup_{H\in\mathfrak{h}_0}|\phi(H;d)|$$

for $F\in C^\infty(\mathfrak{g}_0)$, $\phi\in C^\infty(\mathfrak{h})$, $D\in\mathfrak{D}(\mathfrak{g})$ and $d\in\mathfrak{D}(\mathfrak{h})$. We claim that for any $D\in\mathfrak{D}(\mathfrak{g})$, we can select a finite number of elements $d_1,\cdots,d_N\in\mathfrak{D}(\mathfrak{h})$ such that

$$\nu_D(\psi_g)\leqq\sum_{i=1}^N\sigma_{d_i}(g)$$

for $g\in J(\mathfrak{h}_0)$. It is enough to prove this for $D=p\partial(q)$ $(p,q\in S(\mathfrak{g}))$. We shall use induction on the degree of q which we denote by m. If $m=0$, we may assume that $D=p$. Since G is compact, the Casimir polynomial ω is a negative-definite quadratic form on $\mathfrak{g}_0$, and so it is clear that we can

[11] $(-1)^{k/2}=((-1)^{\frac{1}{2}})^k$ for any integer k.

select $p_0 \in I(\mathfrak{g})$ such that p_0 takes only real nonnegative values on $\mathfrak{g}_0$ and $|p(X)| \leqq p_0(X)$ $(X \in \mathfrak{g}_0)$. Then $p_0\psi_g = \psi_{\bar{p}_0 g}$, and therefore $\nu_D(\psi_g) \leqq \nu_{p_0}(\psi_g) = \nu_1(\psi_{\bar{p}_0 g})$. From Lemma 1 and its Corollary, there exist elements $p_1 \in S(\mathfrak{h})$ and $d \in \mathfrak{D}(\mathfrak{h})$ such that $(\bar{p}_0\phi)^{\sim} = \partial(p_1)\tilde{\phi}$ and

$$\int_{\mathfrak{h}_0} |\pi\partial(\pi p_1)\tilde{\phi}|\, dH \leqq \sigma_d(\phi)$$

for $\phi \in \mathcal{B}(\mathfrak{h}_0)$. Therefore

$$\nu_D(\psi_g) \leqq \nu_1(\psi_{\bar{p}_0 g}) \leqq \int |\pi\partial(\pi p_1)\tilde{g}|\, dH \leqq \sigma_d(g) \qquad (g \in J(\mathfrak{h}_0))$$

since $|\xi(X:Y)| \leqq 1$ $(X, Y \in \mathfrak{g}_0)$. Now suppose $m \geqq 1$. Again choose $p_0 \in I(\mathfrak{g})$ such that $|p(X)| \leqq p_0(X)$ for $X \in \mathfrak{g}_0$. Then if $D_0 = p_0\partial(q)$, it is obvious that $\nu_D(\psi_g) \leqq \nu_{D_0}(\psi_g)$. Also, it is clear that

$$D_0 = \partial(q) \circ p_0 + \sum_{i=1}^{k} p_i\partial(q_i),$$

where k is some integer, $p_i, q_i \in S(\mathfrak{g})$ and the degree of each q_i is smaller than m. In view of the induction hypothesis, it is sufficient to prove our statement for $\Delta = \partial(q) \circ p_0$. But $\Delta\psi_g = \partial(q)\psi_{g_0}$, where $g_0 = \bar{p}_0 g$, and

$$\xi(X;\partial(q):Y) = \int_G \hat{q}(xY)\eta'(X:xY)\,dx \qquad (X, Y \in \mathfrak{g}_0).$$

We again select $q_0 \in I(\mathfrak{g})$ such that $|\hat{q}(X)| \leqq q_0(X)$ for $X \in \mathfrak{g}_0$. Then $|\xi(X;\partial(q):Y)| \leqq q_0(Y)$ $(X, Y \in \mathfrak{g}_0)$, and therefore

$$|\psi_{g_0}(X;\partial(q))| \leqq \int_{\mathfrak{h}_0} |\bar{q}_0\pi\partial(\pi)\tilde{g}_0|\, dH.$$

Choose $p_1 \in S(\mathfrak{h})$ and $d \in \mathfrak{D}(\mathfrak{h})$ such that $(\bar{p}_0\phi)^{\sim} = \partial(p_1)\tilde{\phi}$ and

$$\int_{\mathfrak{h}_0} |\bar{q}_0\pi\partial(\pi p_1)\tilde{\phi}|\, dH \leqq \sigma_d(\phi)$$

for $\phi \in \mathcal{B}(\mathfrak{h})$. Then $\nu_\Delta(\psi_g) = \nu_{\partial(q)}(\psi_{g_0}) \leqq \sigma_d(g)$ $(g \in J(\mathfrak{h}_0))$.

The above result shows that if $g \in J(\mathfrak{h}_0)$, then ψ_g lies in $J(\mathfrak{g}_0)$ and[12] $\psi' : g \rightarrow (c')^{-1}\psi_g$ is a continuous mapping of $J(\mathfrak{h}_0)$ into $J(\mathfrak{g}_0)$. On the other hand, it is obvious that if $f \in J(\mathfrak{g}_0)$, then $\bar{f} \in J(\mathfrak{h}_0)$ and the mapping $\tau : f \rightarrow \bar{f}$ of $J(\mathfrak{g}_0)$ into $J(\mathfrak{h}_0)$ is continuous and univalent. Since $\tau(\psi_g) = c'g$, it follows that $\psi_{\bar{f}} = c'f$ and therefore these two mappings τ and ψ' are inverses of each other. Hence the theorem.

The following result will be needed in Section 8.

---

[12] We shall prove in Section 6 that $\langle\pi, \pi\rangle \neq 0$ (see the Corollary to Lemma 18).

LEMMA 17. *For any* $f \in \mathcal{B}(\mathfrak{h}_0)$ *there exists a unique element* Ψ_f *in* $J(\mathfrak{h}_0)$ *such that*

$$\pi(H)\Psi_f(H) = \sum_{s \in W} \epsilon(s) f(sH) \qquad (H \in \mathfrak{h}_0).$$

Moreover $f \to \Psi_f$ *is a continuous mapping of* $\mathcal{B}(\mathfrak{h}_0)$ *into* $J(\mathfrak{g}_0)$.

Put

$$\Psi_f(X) = c_1 \int_{\mathfrak{h}_0} \xi(X:H)\pi(H) \sum_{s \in W} \epsilon(s)\bar{f}(sH)\,dH \qquad (f \in \mathcal{B}(\mathfrak{h}_0), X \in \mathfrak{g}_0),$$

where $\bar{f}$ is the Fourier transform of f and[12] $c_1 = \langle \pi, \pi \rangle^{-1}$. Then it follows from Theorem 2 that

$$\pi(H')\Psi_f(H') = \sum_{s \in W} \epsilon(s) f(sH') \qquad (H' \in \mathfrak{h}_0).$$

Furthermore, we show exactly as above that $\Psi_f \in J(\mathfrak{g}_0)$ and the mapping $f \to \Psi_f$ is continuous. Finally, since $\mathfrak{g}_0 = \bigcup_{x \in G} x\mathfrak{h}_0$, every invariant function in $C^\infty(\mathfrak{g}_0)$ is uniquely determined by its restriction on $\mathfrak{g}_0'$. This proves the uniqueness of Ψ_f.

6. Some further results. We now discard the assumption about the compactness of G. Define δ as in Theorem 1, and, for $\xi \in \mathfrak{D}(\mathfrak{g})$ and $\eta \in \mathfrak{D}(\mathfrak{h})$, let ξ_0 and η_0 denote their respective local expressions at zero. It is clear that if $\xi \in \mathfrak{J}(\mathfrak{g})$, then $\xi_0 \in \partial(I(\mathfrak{g}))$.

LEMMA 18. $(\partial(\pi) \circ \delta(\xi))_0 = (\partial(\pi) \circ \delta(\xi_0))_0$ *for every* $\xi \in \mathfrak{J}(\mathfrak{g})$.

It is known (see Mostow [7]) that we can find a compact real form $\mathfrak{u}$ of $\mathfrak{g}$ such that $\mathfrak{h} \cap \mathfrak{u}$ is a Cartan subalgebra of $\mathfrak{u}$. Let G_c be the (connected) complex adjoint group of $\mathfrak{g}$ and U the (connected) adjoint group of $\mathfrak{u}$. Then both G and U are real analytic subgroups of G_c corresponding to the real subalgebras $\mathfrak{g}_0$ and $\mathfrak{u}$ of $\mathfrak{g}$. Then (see Section 2) G_c operates on $\mathfrak{D}(\mathfrak{g})$, and it is clear that $I(\mathfrak{g})$ is exactly the algebra of those polynomials p on $\mathfrak{g}$ which are invariant under G_c. Therefore the two algebras $\mathfrak{J}(\mathfrak{g})$ and $\mathfrak{J}(\mathfrak{h})$ are the same whether we start from the real form $\mathfrak{g}_0$ or $\mathfrak{u}$. Let du denote the normalized Haar measure of U, and for any $f \in C^\infty(\mathfrak{u})$ define

$$\phi_f(H) = \pi(H) \int_U f(uH)\,du \qquad (H \in \mathfrak{h} \cap \mathfrak{u})$$

as in Section 5. In order to prove the lemma, let us first suppose that $\xi_0 = 0$. Then from Lemma 16, $\phi_{\xi f}(0;\partial(\pi)) = 0$ for all $f \in C^\infty(\mathfrak{u})$. But we know (Lemma 15) that $\phi_{\xi f} = \delta(\xi)\phi_f$. This proves that $\partial(\pi)(\delta(\xi)\phi_f)$ has

the value zero at the origin. Now suppose $f \in I(\mathfrak{g})$. Then $\phi_f = \pi \bar{f}$, where $\bar{f}$ is the restriction of f on $\mathfrak{h} \cap \mathfrak{u}$. Hence we conclude from Lemma 9 that $(\partial(\pi) \circ \delta(\xi))(\pi p)$ takes the value zero at the origin for every $p \in I(\mathfrak{h})$. Select $q \in S(\mathfrak{h})$ such that $(\partial(\pi) \circ \delta(\xi))_0 = \partial(q)$. Since $\delta(\xi)$ is invariant under W, it is obvious that $q^s = \epsilon(s) q$ $(s \in W)$. We claim $q = 0$. For otherwise we could select $p_1 \in S(\mathfrak{h})$ such that $\langle q, p_1 \rangle \neq 0$. But $\langle q, p_1 \rangle = \langle q^s, p_1^s \rangle = \epsilon(s) \langle q, p_1^s \rangle$ $(s \in W)$. Hence $\langle q, p_2 \rangle = \langle q, p_1 \rangle \neq 0$, where $p_2 = w^{-1} \sum_{s \in W} \epsilon(s) p_1^s$. However it follows from Lemma 10 that $p_2 = \pi p$ for some $p \in I(\mathfrak{h})$, and therefore $\langle q, \pi p \rangle \neq 0$. On the other hand, in view of the definition of q, $\langle q, \pi p \rangle$ is exactly the value of $(\partial(\pi) \circ \delta(\xi))(\pi p)$ at the origin, which, as we have seen above, must be zero. This contradiction proves that $q = 0$, and therefore $(\delta(\pi) \circ \delta(\xi))_0 = 0$. The general case is reduced to the one discussed above by replacing ξ by $\xi - \xi_0$.

Let $\bar{\theta}$ denote the conjugation of $\mathfrak{g}$ with respect to $\mathfrak{u}$, and $p \to p_*$ $(p \in S(\mathfrak{g}))$ the automorphism of $S(\mathfrak{g})$ over R which coincides with $-\bar{\theta}$ on $\mathfrak{g}$. Select a base $X_1, \cdots, X_n$ for $\mathfrak{u}$ over R such that $B(X_i, X_j) = -\delta_{ij}$, $1 \leqq i, j \leqq n$. Then if

$$p = \sum_{m_i \geqq 0} a(m_1, \cdots, m_n) X_1^{m_1} \cdots X_n^{m_n} \qquad (a(m_1, \cdots, m_n) \in C),$$

it is clear that $\langle p_*, p \rangle = \sum_{m_i \geqq 0} m_1! \cdots m_n! \, |a(m_1, \cdots, m_n)|^2 > 0$ unless $p = 0$. On the other hand, since every root α takes only pure imaginary values on $\mathfrak{h} \cap \mathfrak{u}$, it is obvious that $\pi_* = \pi$. Therefore $\langle \pi^k, \pi^k \rangle$ is a positive real number for every integer $k \geqq 0$. Moreover, since $\pi^2 \in I(\mathfrak{h})$, there exists (Lemma 9) a unique element $\eta \in I(\mathfrak{g})$ such that $\bar{\eta} = \pi^2$. It is clear that η_* is also in $I(\mathfrak{g})$ and $\bar{\eta}_* = (\pi^2)_* = \pi^2 = \bar{\eta}$. Hence we conclude from Lemma 9 that $\eta_* = \eta$, and therefore $\langle \eta^k, \eta^k \rangle > 0$ for any integer $k \geqq 0$. Put $\xi = \partial(\eta^k) \circ \eta^k$ for some fixed k. It is obvious that $\xi_0 = \langle \eta^k, \eta^k \rangle$, and therefore we get the following Corollary from Lemma 18.

Corollary. *Put $\xi = \partial(\eta^k) \circ \eta^k$ for some integer $k \geqq 0$. Then*

$$(\partial(\pi) \circ \delta(\xi))_0 = \langle \eta^k, \eta^k \rangle \partial(\pi).$$

Moreover, $\langle \eta^k, \eta^k \rangle$ and $\langle \eta^k, \eta^k \rangle$ are positive real numbers.

We shall now prove an algebraic result which will be needed in another paper. As before let ω denote the Casimir polynomial of $\mathfrak{g}$ and define a differential operator σ on $\mathfrak{g}_0$ as follows: $f(X; \sigma) = f(X; \partial(X))$ $(X \in \mathfrak{g}_0$, $f \in C^\infty(\mathfrak{g}_0))$. It is obvious that $\sigma \in \mathfrak{D}(\mathfrak{g})$.

Lemma 19. *For any integer $k \geqq 1$,*

$$\partial(\omega^k)\circ\omega^k \equiv 4^k k!(\tfrac{1}{2}n+\sigma+k-1)(\tfrac{1}{2}n+\sigma+k-2)\cdots(\tfrac{1}{2}n+\sigma) \mod \omega\mathfrak{D}(\mathfrak{g}),$$

where $n=\dim_C \mathfrak{g}$.

Define $\{D_1, D_2\} = D_1D_2 - D_2D_1$ as before for any two differential operators D_1, D_2. Then a simple calculation shows that $\{\partial(\omega), \omega\} = 2n+4\sigma$. Moreover, if p is a homogeneous polynomial in $S(\mathfrak{g})$ of degree m, it is easily seen that $\sigma p = mp$, and therefore it is clear that $\partial(\omega)\sigma = (\sigma+2)\partial(\omega)$. Hence

$$\begin{aligned}\{\partial(\omega^k),\omega\} &= \sum_{0\leqq m<k}\partial(\omega^{k-1-m})(2n+4\sigma)\partial(\omega^m)\\ &= \sum_{0\leqq m<k}(2n+4(\sigma+2k-2-2m))\partial(\omega^{k-1})\\ &= 4k(\tfrac{1}{2}n+\sigma+k-1)\partial(\omega^{k-1}).\end{aligned}$$

Therefore

$$\partial(\omega^k)\circ\omega^k \equiv \{\partial(\omega^k),\omega\}\circ\omega^{k-1} \equiv 4k(\tfrac{1}{2}n+\sigma+k-1)\partial(\omega^{k-1})\circ\omega^{k-1} \mod \omega\mathfrak{D}(\mathfrak{g}),$$

and our assertion now follows by induction.

This lemma has the following significance for our later applications. Let t denote a real variable.

COROLLARY. *For any* $f\in C_c^\infty(\mathfrak{g}_0)$, *put* $f_k=\partial(\omega^k)(\omega^k f)$ $(k\geqq 0)$. *Then if* $X\neq 0$ *is an element in* $\mathfrak{g}_0$ *such that* $\omega(X)=0$, *we have*[13]

$$\int_0^\infty f_k(tX)dt = 4^k k!\{\Gamma(\tfrac{1}{2}n+k-1)/\Gamma(\tfrac{1}{2}n-1)\}\int_0^\infty f(tX)dt$$

for all integers $k\geqq 0$.

It is obvious that $g(tX;\sigma)=tg(tX;\partial(X))=t(d/dt)g(tX)$ for any $g\in C_c^\infty(\mathfrak{g}_0)$. Hence

$$\int_0^\infty g(tX;\sigma+1)dt=\int_0^\infty (d/dt)(tg(tX))dt=0.$$

On the other hand, it follows from Lemma 19 that

$$f_k = c_k f + (\sigma+1)g_1 + \omega g_2,$$

where $g_1, g_2\in C_c^\infty(\mathfrak{g})$ and $c_k=4^k k!\,\Gamma(\tfrac{1}{2}n+k-1)/\Gamma(\tfrac{1}{2}n-1)$. Therefore, since $\omega(tX)=t^2\omega(X)=0$, we conclude that

$$\int_0^\infty f_k(tX)dt = c_k\int_0^\infty f(tX)dt.$$

[13] Here Γ stands for the classical Gamma function.

7. Differential operators on a reductive subalgebra. Let $\mathfrak{m}_0$ be a Lie subalgebra of $\mathfrak{g}_0$. We assume that $\mathfrak{m}_0 \supset \mathfrak{h}_0$ and $\mathfrak{m}_0$ is reductive in $\mathfrak{g}_0$ (see Koszul [6]). Then we can select a subspace $\mathfrak{q}_0$ of $\mathfrak{g}_0$ such that $[\mathfrak{m}_0, \mathfrak{q}_0] \subset \mathfrak{q}_0$ and $\mathfrak{g}_0$ is the direct sum of $\mathfrak{m}_0$ and $\mathfrak{q}_0$. Let $\mathfrak{m}, \mathfrak{q}$ be the complexification of $\mathfrak{m}_0, \mathfrak{q}_0$, respectively, in $\mathfrak{g}$ and let Q be the set of all roots $\alpha \in P$ for which $X_\alpha \in \mathfrak{m}$. Then it is clear that $\mathfrak{m} = \mathfrak{h} + \sum_{\alpha \in Q} (CX_\alpha + CX_{-\alpha})$ and $\mathfrak{q} = \sum_{\alpha \in Q'} (CX_\alpha + CX_{-\alpha})$, where Q' is the complement of Q in P. Since the restriction of the bilinear form B on $\mathfrak{m}$ is obviously nondegenerate, we can apply the formalism described in Section 2 to $E_0 = \mathfrak{g}_0$ and $F_0 = \mathfrak{m}_0$. For any $X \in \mathfrak{m}$, let $\zeta(X)$ denote the determinant of the restriction of $\operatorname{ad} X$ on $\mathfrak{q}$. (If $\mathfrak{q} = \{0\}$, we define $\zeta(X)$ to be 1.) Then ζ, being a polynomial function on $\mathfrak{m}$, lies in $S(\mathfrak{m})$. Moreover, ζ coincides on $\mathfrak{h}$ with $(-1)^s \prod_{\alpha \in Q'} \alpha^2$, where s is the number of roots in Q'. Hence $\zeta \neq 0$. Let $\mathfrak{m}_0'$ denote the set of all $X \in \mathfrak{m}_0$ where $\zeta(X) \neq 0$. Then $\mathfrak{m}_0'$ is an open dense subset of $\mathfrak{m}_0$ and $\mathfrak{h}_0' \subset \mathfrak{m}_0'$. Put $\mathfrak{Q} = \lambda(S(\mathfrak{q}))$, where λ is the canonical mapping of $S(\mathfrak{g})$ into $\mathfrak{B}$. The next two lemmas are proved in the same way as Lemmas 4 and 5.

LEMMA 20. *If $X \in \mathfrak{m}_0'$, Γ_X defines a one-one mapping of $\mathfrak{Q} \times S(\mathfrak{m})$ onto $S(\mathfrak{g})$.*

LEMMA 21. *For every $p \in S(\mathfrak{g})$, there exists an integer $k \geqq 0$ and a polynomial mapping γ_p of $\mathfrak{m}$ into $\mathfrak{Q} \times S(\mathfrak{m})$ such that $\Gamma_X(\gamma_p(X)) = \zeta(X)^k p$ $(X \in \mathfrak{m}_0)$.*

For any $x \in G$, let $b \to b^x$ $(b \in \mathfrak{B})$ denote the unique antomorphism of $\mathfrak{B}$ which coincides with x on $\mathfrak{g}$. Then we also get an automorphism $\mu \to \mu^x$ of $\mathfrak{B} \times S(\mathfrak{g})$ given by $(b \times p)^x = b^x \times p^x$ $(b \in \mathfrak{B}, p \in S(\mathfrak{g}))$. It is obvious from the definition of Γ_Y $(Y \in \mathfrak{g}_0)$ that $(\Gamma_Y(\mu))^x = \Gamma_{xY}(\mu^x)$ $(\mu \in \mathfrak{B} \times S(\mathfrak{g}))$. Let M be the analytic subgroup of G corresponding to $\mathfrak{m}_0$. It is obvious that $\zeta^m = \zeta$, and therefore $m\mathfrak{m}_0' = \mathfrak{m}_0'$ $(m \in M)$. For any $p \in S(\mathfrak{g})$, let $\beta_p(X)$ $(X \in \mathfrak{m}_0')$ denote the unique element in $\mathfrak{Q} \times S(\mathfrak{m})$ (see Lemma 20) such that $\Gamma_X(\beta_p(X)) = p$. Then if $m \in M$,

$$p^m = (\Gamma_X(\beta_p(X)))^m = \Gamma_{mX}(\beta_p(X)^m) \qquad (X \in \mathfrak{m}_0').$$

and this shows that $\beta_{p^m}(mX) = (\beta_p(X))^m$. Thus we have obtained the following result.

LEMMA 22. *For any $p \in S(\mathfrak{g})$ and $X \in \mathfrak{m}_0'$, let β_p denote the unique*

element in $\mathfrak{Q} \times S(\mathfrak{m})$ *such that* $\Gamma_X(\beta_p(X)) = p$. *Then* $\beta_{p^m}(mX) = (\beta_p(X))^m$ $(m \in M)$.

Put $\mathfrak{Q}' = \sum_{d \geqq 1} \lambda(S_d(\mathfrak{q}))$, where $S_d(\mathfrak{q})$ is the space of homogeneous elements in $S(\mathfrak{q})$ of degree d. Let $\mu_X(p)$ $(X \in \mathfrak{m}_0', p \in S(\mathfrak{g}))$ denote the unique element in $S(\mathfrak{m})$ such that $\beta_p(X) - (1 \times \mu_X(p)) \in \mathfrak{Q}' \times S(\mathfrak{m})$. Then it follows from Lemma 21 that there exists a differential operator $\Delta(p)$ on $\mathfrak{m}_0'$ whose local expression at X coincides with $\partial(\mu_X(p))$. On the other hand, since ζ is nowhere zero on $\mathfrak{m}_0'$, $|\zeta|^{\frac{1}{2}}$ and $|\zeta|^{-\frac{1}{2}}$ are analytic functions on $\mathfrak{m}_0'$, and so, for any $q \in S(\mathfrak{m})$, $|\zeta|^{-\frac{1}{2}}\partial(q) \circ |\zeta|^{\frac{1}{2}}$ is a well-defined differential operator on $\mathfrak{m}_0'$. Let $p_{\mathfrak{m}}$ denote the restriction of a polynomial $p \in S(\mathfrak{g})$ on $\mathfrak{m}$. Then $p_{\mathfrak{m}} \in S(\mathfrak{m})$ and $\Delta(p) - |\zeta|^{-\frac{1}{2}}\partial(p_{\mathfrak{m}}) \circ |\zeta|^{\frac{1}{2}}$ is a differential operator on $\mathfrak{m}_0'$. We shall denote its local expression at $X \in \mathfrak{m}_0'$ in the usual way by $(\Delta(p) - |\zeta|^{-\frac{1}{2}}\partial(p_{\mathfrak{m}}) \circ |\zeta|^{\frac{1}{2}})_X$. Let $\mathfrak{M}$ be the subalgebra of $\mathfrak{B}$ generated by $(1, \mathfrak{m})$. We put $\mathfrak{M}' = \mathfrak{M}\mathfrak{m}$.

LEMMA 23. *If* $p \in I(\mathfrak{g})$ *and* $X \in \bigcup_{m \in M} m\mathfrak{h}_0'$, *then*

$$(\Delta(p) - |\zeta|^{-\frac{1}{2}}\partial(p_{\mathfrak{m}}) \circ |\zeta|^{\frac{1}{2}})_X \in \partial(\Gamma_X(\mathfrak{M}' \times S(\mathfrak{m}))).$$

Let $D = \Delta(p) - |\zeta|^{-\frac{1}{2}}\partial(p_{\mathfrak{m}}) \circ |\zeta|^{\frac{1}{2}}$. Since both ζ and $p_{\mathfrak{m}}$ are invariant under M, it follows from Lemma 22 that $D_{mX} = (D_X)^m$ $(m \in M, X \in \mathfrak{m}_0')$. Hence it would be sufficient to prove that D_H lies in $\partial(\Gamma_H(\mathfrak{M}' \times S(\mathfrak{m})))$ for $H \in \mathfrak{h}_0'$. Since $\mathfrak{m}_0$ is reductive, it is clear that Lemma 4 can be applied to $\mathfrak{m}_0$ in place of $\mathfrak{g}_0$. We now use the notation of Section 3 and put $\mathfrak{S}_{\mathfrak{m}} = \mathfrak{S} \cap \mathfrak{M}$ and $\mathfrak{S}_{\mathfrak{m}}' = \mathfrak{S}' \cap \mathfrak{M}$. Also fix an element $H_0 \in \mathfrak{h}_0'$. Since $S(\mathfrak{s}) \cap S(\mathfrak{m}) = S(\mathfrak{s} \cap \mathfrak{m})$ and the canonical mapping λ of $S(\mathfrak{g})$ onto $\mathfrak{B}$ is a linear isomorphism, it follows that $\lambda(S(\mathfrak{s} \cap \mathfrak{m})) = \mathfrak{S}_{\mathfrak{m}}$ and $\mathfrak{S}_{\mathfrak{m}}' = \mathfrak{S} \cap \mathfrak{M}'$. Therefore from Lemma 4 (applied to $\mathfrak{m}_0$), Γ_{H_0} defines a one-one mapping of $\mathfrak{S}_{\mathfrak{m}} \times S(\mathfrak{h})$ into $S(\mathfrak{m})$. Moreover $\zeta(H)$ is real and equal to $\pm \prod_{\alpha \in Q'} (\alpha(H))^2$ if $H \in \mathfrak{h}_0$. Therefore by applying Lemmas 7 and 8 to $\mathfrak{m}_0$ (instead of $\mathfrak{g}_0$), we conclude that

$$(|\zeta|^{-\frac{1}{2}}\partial(p_{\mathfrak{m}}) \circ |\zeta|^{\frac{1}{2}})_{H_0} - (\pi^{-1}\partial(\bar{p}) \circ \pi)_{H_0} \in \partial(\Gamma_{H_0}(\mathfrak{S}_{\mathfrak{m}}' \times S(\mathfrak{h}))),$$

where $\bar{p}$ is the restriction of p (and therefore also of $p_{\mathfrak{m}}$) on $\mathfrak{h}$. On the other hand, it follows from the definition of $\Delta(p)$ that

$$(\Delta(p))_{H_0} - \partial(p) \in \partial(\Gamma_{H_0}(\mathfrak{Q}' \times S(\mathfrak{m}))).$$

Therefore

$$D_{H_0} \equiv \partial(p) - (\pi^{-1}\partial(\bar{p}) \circ \pi)_{H_0} \equiv 0 \mod \partial(\Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{m})))$$

from Lemma 8. Now it is an immediate consequence of the defintion of Γ_Y $(Y \in \mathfrak{g}_0)$ that $\Gamma_Y(b_1 b_2 \times q) = \Gamma_Y(b_1 \times \Gamma_Y(b_2 \times q))$ $(b_1, b_2 \in \mathfrak{B}, q \in S(\mathfrak{g}))$. Therefore, since $S(\mathfrak{m}) = \Gamma_{H_0}(\mathfrak{S}_\mathfrak{m} \times S(\mathfrak{h}))$, it follows that $\Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{m})) \subset \Gamma_{H_0}(\mathfrak{B}' \times S(\mathfrak{h}))$, where $\mathfrak{B}' = \mathfrak{B}\mathfrak{g}$. But $\mathfrak{B}' = \mathfrak{S}' + \mathfrak{B}\mathfrak{h}$ and $\Gamma_{H_0}(\mathfrak{B}\mathfrak{h} \times S(\mathfrak{h})) = \{0\}$. Therefore $\Gamma_{H_0}(\mathfrak{B}' \times S(\mathfrak{h})) = \Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{h}))$. This proves that $\Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{m})) = \Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{h}))$, and hence $D_{H_0} \in \partial(S(\mathfrak{m}) \cap \Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{h})))$. But, as we have seen,, $S(\mathfrak{m}) = \Gamma_{H_0}(\mathfrak{S}_\mathfrak{m} \times S\text{A}\mathfrak{h}))$ and Γ_{H_0} is univalent on $\mathfrak{S} \times S(\mathfrak{h})$ (Lemma 4). Therefore

$$D_{H_0} \in \partial(\Gamma_{H_0}(\mathfrak{S}_\mathfrak{m}' \times S(\mathfrak{h})) \subset \partial(\Gamma_{H_0}(\mathfrak{M}' \times S(\mathfrak{m}))),$$

and so the lemma is proved.

COROLLARY. *If* $H \in \mathfrak{h}_0'$ *then*

$$(\Delta(p))_H - (\pi^{-1}\partial(\bar{p}) \circ \pi)_H \in \partial(\Gamma_H(\mathfrak{M}' \times S(\mathfrak{h})))$$

for $p \in I(\mathfrak{g})$.

For, in view of what we have seen above, the left side lies in

$$\partial(S(\mathfrak{m}) \cap \Gamma_H(\mathfrak{S}' \times S(\mathfrak{m}))) \quad \text{and} \quad S(\mathfrak{m}) \cap \Gamma_H(\mathfrak{S}' \times S(\mathfrak{m})) \subset \Gamma_H(\mathfrak{M}' \times S(\mathfrak{h})).$$

8. Closer study of a special case. Define $\mathfrak{k}_0$ and $\mathfrak{p}_0$ as in [4(c), §2] adn let $\mathfrak{k}, \mathfrak{p}$ denote their respective complexifications in $\mathfrak{g}$. *Throughout this section we shall assume that* $\mathfrak{h}_0 \subset \mathfrak{k}_0$. Then the theory developed in Section 7 can be applied to $\mathfrak{m}_0 = \mathfrak{k}_0$. In this case $\mathfrak{q}_0 = \mathfrak{p}_0$ and $\zeta(X) = \det(\operatorname{ad} X)_\mathfrak{p}$ $(X \in \mathfrak{k})$, where $(\operatorname{ad} X)_\mathfrak{p}$ is the restriction of $\operatorname{ad} X$ on $\mathfrak{p}$. Put $\mathfrak{P} = \lambda(S(\mathfrak{p}))$. Then we intend to prove the following result concerning the Casimir polynomial ω of $\mathfrak{g}$.

LEMMA[14] 24. *There exists a unique polynomial mapping* γ_ω *of* $\mathfrak{k}$ *into* $\mathfrak{P} \times S(\mathfrak{k})$ *such that* $\Gamma_X(\gamma_\omega(X)) = \zeta(X)\omega$ $(X \in \mathfrak{k}_0)$. *Moreover* $(\gamma_\omega(X))^k = \gamma_\omega(kX)$ *for* $k \in K$ *and* $X \in \mathfrak{k}$.

The case $\mathfrak{g}_0 = \mathfrak{k}_0$ being trivial, we assume that $\mathfrak{p}_0 \neq 0$. Let P_- and P_0 be the sets of all compact and all noncompact roots in P, respectively (see [4(g), p. 751]). Then if r is the number of roots in P_0, $\dim \mathfrak{p} = 2r$. Let t be an indeterminate and consider the polynomial

$$\prod_{\beta \in P_0} (t - \beta^2) = t^r + q_1 t^{r-1} + \cdots + q_r$$

with coefficients $q_i \in S(\mathfrak{h})$. Let $W_\mathfrak{k}$ be the subgroup of the Weyl group W

[14] The results of this section are quite similar to those of [4(e), §10].

generated by the reflexions s_α corresponding to $\alpha \in P_-$. Then, since $\mathfrak{k}$ is reductive (Lemma 5 of [4(c)]), $W_{\mathfrak{k}}$ can also be regarded as the Weyl group of $\mathfrak{k}$ with respect to $\mathfrak{h}$ (see [4(e), §6]). Let K denote the analytic subgroup of G corresponding to $\mathfrak{k}_0$ and $I(\mathfrak{k})$ the set of those $p \in S(\mathfrak{k})$ which are invariant under K. Similarly, let $I_{\mathfrak{k}}(\mathfrak{h})$ be the set of all elements in $S(\mathfrak{h})$ which are invariant under $W_{\mathfrak{k}}$. Then Chevalley's Theorem (Lemma 9) is obviously applicable to $(\mathfrak{k}, \mathfrak{h})$ in place of $(\mathfrak{g}, \mathfrak{h})$. Hence $p \rightarrow \bar{p}$ $(p \in I(\mathfrak{k}))$ is an isomorphism of $I(\mathfrak{k})$ onto $I_{\mathfrak{k}}(\mathfrak{h})$. Now if β is a noncompact root and $s \in W_{\mathfrak{k}}$, then $s\beta$ is also noncompact (see the proof of Lemma 10 of [4(g)]). From this it follows that $q_i \in I_{\mathfrak{k}}(\mathfrak{h})$, $1 \leqq i \leqq r$. Hence we can select $\sigma_i \in I(\mathfrak{k})$ such that $q_i = \bar{\sigma}_i$. For any $X \in \mathfrak{k}$, put $S(X) = (\operatorname{ad} X)_{\mathfrak{p}}{}^2$. Then we shall first prove the following lemma.

LEMMA 25. *$\sigma_r = \zeta$ and*

$$(S(X))^r + \sigma_1(X)(S(X))^{r-1} + \cdots + \sigma_r(X) I_{\mathfrak{p}} = 0 \qquad (X \in \mathfrak{k}).$$

(Here $I_{\mathfrak{p}}$ is the identity mapping of $\mathfrak{p}$.)

It is clear that $\zeta \in I(\mathfrak{k})$ and $\bar{\zeta} = (-1)^r \prod_{\beta \in P_0} \beta^2 = q_r$. Therefore, in view of the above *isomorphism* of $I(\mathfrak{k})$ onto $I_{\mathfrak{k}}(\mathfrak{h})$, we can conclude that $\zeta = \sigma_r$. Moreover $\tau : X \rightarrow \{(S(X))^r + \sigma_1(X)(S(X))^{r-1} + \cdots + \sigma_r(X) I_{\mathfrak{p}}\}$ $(X \in \mathfrak{k})$ is obviously a polynomial mapping of $\mathfrak{k}$ into the space of endomorphisms of $\mathfrak{p}$, and therefore it would be sufficient to prove that τ maps $\mathfrak{k}_0$ into zero. Moreover, since K is compact [7], $\mathfrak{k}_0 = \bigcup_{k \in K} k\mathfrak{h}_0$, and so it would clearly be enough to show that τ maps $\mathfrak{h}_0$ into zero. But if $H \in \mathfrak{h}$, $S(H)$ is semisimple and all its eigenvalues are of the form $\beta(H)^2$ $(\beta \in P_0)$. Therefore

$$\tau(H) = \prod_{\beta \in P_0} (S(H) - \beta(H)^2 I_{\mathfrak{p}}) = 0,$$

and this proves our assertion.

Now put

$$T(X) = -\{(S(X))^{r-1} + \sigma_1(X)(S(X))^{r-2} + \cdots + \sigma_{r-1}(X) I_{\mathfrak{p}}\} \quad (X \in \mathfrak{k}),$$

so that $S(X)T(X) = T(X)S(X) = \zeta(X) I_{\mathfrak{p}}$. Select a base $Y_1, \cdots, Y_p$ $(p = 2r)$ for $\mathfrak{p}$ over C. Since $\mathfrak{k}$ and $\mathfrak{p}$ are orthogonal under B, B is nondegenerate on $\mathfrak{p}$. Hence we can choose $Y_i' \in \mathfrak{p}$ $(1 \leqq i \leqq p)$ such that $B(Y_i', Y_j) = \delta_{ij}$ $(1 \leqq i, j \leqq p)$. Let $\omega_{\mathfrak{k}}$ and $\omega_{\mathfrak{p}}$ denote the restrictions of ω on $\mathfrak{k}$ and $\mathfrak{p}$, respectively. Then in view of the above-mentioned orthogonality of $\mathfrak{k}$ and $\mathfrak{p}$, $\omega = \omega_{\mathfrak{k}} + \omega_{\mathfrak{p}}$. Moreover, it is easy to see that $\omega_{\mathfrak{p}} = \sum_{1 \leqq i \leqq p} Y_i Y_i'$.

Now fix an element $X \in \mathfrak{k}$ and let S', T' be two linear transformations of $\mathfrak{p}$ which commute with $(\operatorname{ad} X)_{\mathfrak{p}}$. Put $U_i = S'Y_i$, $V_i = T'Y_i$, $U_i' = S'Y_i'$, $V_i' = T'Y_i'$ $(1 \leqq i \leqq p)$. Note that $Z = \sum_{1 \leqq i \leqq p} B(Z, Y_i')Y_i = \sum_{1 \leqq i \leqq p} B(Z, Y_i)Y_i'$ $(Z \in \mathfrak{p})$, and therefore $(\operatorname{ad} X)Z = -\sum_i B(Z, (\operatorname{ad} X)Y_i')Y_i$. Hence

$$(\operatorname{ad} X)U_i = S'(\operatorname{ad} X)Y_i = -\sum_j B(Y_i, (\operatorname{ad} X)Y_j')U_j,$$

$$(\operatorname{ad} X)V_i' = T'(\operatorname{ad} X)Y_i' = \sum_j B((\operatorname{ad} X)Y_i', Y_j)V_j',$$

and so if we consider the tensor product $\mathfrak{p} \times \mathfrak{p}$, it follows that

$$\sum_i ((\operatorname{ad} X)U_i) \times V_i' = -\sum_{i,j} B(Y_i, (\operatorname{ad} X)Y_j')U_j \times V_i' = -\sum_j U_j \times (\operatorname{ad} X)V_j'.$$

Obviously, this implies that

$$\sum_i [X, U_i]V_i' = -\sum_i U_i[X, V_i'],$$

$$\sum_i [[X, U_i], V_i'] = -\sum_i [U_i, [X, V_i']].$$

Now put $Y_j(X) = T(X)Y_j$ $(1 \leqq j \leqq p)$ so that $S(X)Y_j(X) = \zeta(X)Y_j$. Then if $U, V \in \mathfrak{p}$ and $X \in \mathfrak{k}_0$,

$$\Gamma_X(U \cdot V \times 1) = (L_{[U,X]} + d_U)[V, X] = [X, U][X, V] - [U, [X, V]]$$

in the notation of Section 3. Hence

$$\sum_{1 \leqq j \leqq p} \Gamma_X(Y_j' \cdot Y_j(X) \times 1) = \sum_j [X, Y_j'][X, Y_j(X)] - \sum_j [Y_j', [X, Y_j(X)]].$$

But since $(\operatorname{ad} X)_{\mathfrak{p}} T(X)$ commutes with $(\operatorname{ad} X)_{\mathfrak{p}}$, it follows from our result above that

$$\sum_j [X, Y_j'][X, Y_j(X)] = -\sum_j Y_j'(S(X)Y_j(X)) = -\zeta(X)\omega_{\mathfrak{p}},$$

and therefore

$$\sum_{1 \leqq j \leqq p} \Gamma_X(Y_j' \cdot Y_j(X) \times 1) = -\zeta(X)\omega_{\mathfrak{p}} - \sum_j [Y_j', [X, Y_j(X)]].$$

Now put $b(X) = -\frac{1}{2} \sum_i (Y_i' \cdot Y_i(X) + Y_i(X) \cdot Y_i')$ $(X \in \mathfrak{k})$. Then $b(X) \in \mathfrak{P}$ and $b(X) = -\sum_j Y_j' \cdot Y_j(X) + \frac{1}{2} \sum_j [Y_j', Y_j(X)]$. Moreover, it follows from our result above that

$$\sum_j [(\operatorname{ad} X)Y_j', Y_j(X)] = -\sum_j [Y_j', (\operatorname{ad} X)Y_j(X)],$$

and therefore $\Gamma_X(b(X)\times 1) = \zeta(X)\omega_{\mathfrak{p}} + \sum_j [Y_j', [X, Y_j(X)]]$ $(X \in \mathfrak{k}_0)$. Put $Z(X) = \sum_j [Y_j', [X, Y_j(X)]]$ and

$$\gamma_\omega(X) = b(X)\times 1 + \zeta(X)(1\times\omega_{\mathfrak{k}}) - (1\times Z(X)) \qquad (X \in \mathfrak{k}).$$

Then $Z(X) \in [\mathfrak{p}, \mathfrak{p}] \subset \mathfrak{k}$, and therefore $\gamma_\omega(X) \in \mathfrak{P}\times S(\mathfrak{k})$. Moreover,

$$\Gamma_X(\gamma_\omega(X)) = \zeta(X)\omega_{\mathfrak{p}} + \zeta(X)\omega_{\mathfrak{k}} = \zeta(X)\omega \qquad (X \in \mathfrak{k}_0)$$

and it is clear from its definition that γ_ω is a polynomial mapping of $\mathfrak{k}$ into $\mathfrak{P}\times S(\mathfrak{k})$. We still have to prove its uniqueness.

Let $\mathfrak{k}_0'$ be the set of all points $X \in \mathfrak{k}_0$ where $\zeta(X) \neq 0$. It follows from Lemma 20 that γ_ω is completely determined on $\mathfrak{k}_0'$ by the condition $\Gamma_X(\gamma_\omega(X)) = \zeta(X)\omega$. But it is obvious that two polynomial mappings of $\mathfrak{k}$ must be identical if they coincide on some nonempty open subset of $\mathfrak{k}_0$. This proves that γ_ω is unique.

For a fixed $k \in K$, consider the mapping $\gamma_\omega' : X \to (\gamma_\omega(kX))^{k^{-1}}$ $(X \in \mathfrak{k})$. It is clear that γ_ω' is a polynomial mapping which, in view of Lemma 22, must coincide with γ_ω on $\mathfrak{k}_0'$. Hence $\gamma_\omega' = \gamma_\omega$, and therefore $(\gamma_\omega(X))^k$ $(k \in K, X \in \mathfrak{k})$. This completes the proof of Lemma 24.

We can now define a differential operator D on $\mathfrak{k}_0$ by

$$D_X = \zeta(X)\partial(\omega_{\mathfrak{k}}) - \partial(Z(X)) \qquad (X \in \mathfrak{k}_0)$$

in the above notation. It is clear that $D \in \mathfrak{D}(\mathfrak{k})$ and it follows from Lemma 24 that D is invariant under K. Finally, it is obvious from the defintion of $\Delta(\omega)$ (in Lemma 23) that $D = \zeta\Delta(\omega)$ on $\mathfrak{k}_0'$. Let D^* denote the adjoint of D.

LEMMA 26. *Let $I^\infty(\mathfrak{k}_0)$ denote the set of all functions $f \in C^\infty(\mathfrak{k}_0)$ which are invariant under K. Then $Df = D^*f$ for $f \in I^\infty(\mathfrak{k}_0)$.*

Let f be a fixed element in $I^\infty(\mathfrak{k}_0)$. We have to prove that $Df - D^*f = 0$. Since D is invariant under K, the same holds for D^*, and therefore $Df - D^*f$ lies in $I^\infty(\mathfrak{k}_0)$. Hence, in view of the fact that $\mathfrak{k}_0 = \bigcup_{k \in K} (k\mathfrak{h}_0)$, it would be enough to prove that $Df - D^*f$ is zero on $\mathfrak{h}_0'$. Let H_0 be any point in $\mathfrak{h}_0'$ and select an open connected neighborhood U of H_0 in $\mathfrak{h}_0'$. Then $V = \bigcup_{k \in K} (kU)$ is an open connected neighborhood of H_0 in $\mathfrak{k}_0$. Let dX denote the Euclidean measure on $\mathfrak{k}_0$. It is obvious that if $g \in C_c^\infty(V)$,

$$\int_V (Df - D^*f)g\, dX = \int_V (Df - D^*f)g_1\, dX,$$

where $g_1(X) = \int_K g(kX)dk$ $(X \in V)$ and dk is the normalized Haar measure on K. Therefore, in order to prove that $Df - D^*f$ is zero on V, it is sufficient to show that

$$\int (Df)\phi\, dX = \int f(D\phi)dX$$

for every $\phi \in I^\infty(\mathfrak{k}_0)$ which vanishes outside some compact set in V. Fix such a function ϕ. Now $V \subset \mathfrak{k}_0'$ and therefore $D = \zeta\Delta(\omega)$ on V. Moreover since ζ takes only nonzero real values on the connected set V, it must keep constant sign. Hence it follows from Lemma 23 that

$$\psi(X;D) = \epsilon\psi(X;|\zeta|^{\frac{1}{2}}\partial(\omega_{\mathfrak{k}})\circ|\zeta|^{\frac{1}{2}}) \qquad (X \in V, \psi \in I^\infty(\mathfrak{k}_0)),$$

where $\epsilon = 1$ or -1 according as ζ is positive or negative on V. Therefore, if $f' = |\zeta|^{\frac{1}{2}}f$ and $\phi' = |\zeta|^{\frac{1}{2}}\phi$, we have only to show that

$$\int (\partial(\omega_{\mathfrak{k}})f')\phi'\, dX = \int f'(\partial(\omega_{\mathfrak{k}})\phi')dX.$$

But, $\omega_{\mathfrak{k}}$ being a homogeneous polynomial of degree 2, $\partial(\omega_{\mathfrak{k}})$ is self-adjoint. Moreover, $\phi' \in C_c^\infty(V)$ and f' is of class C^∞ on V. Therefore the above relation is obvious, and so the lemma is proved.

Since every root α takes only pure imaginary values on $\mathfrak{h}_0$, it is clear that the corresponding Weyl reflexion s_α maps $\mathfrak{h}_0$ into itself. Hence $s\mathfrak{h}_0 = \mathfrak{h}_0$ for any $s \in W$. Put $J(\mathfrak{k}_0) = I^\infty(\mathfrak{k}_0) \cap \mathcal{C}(\mathfrak{k}_0)$ and consider the $\mathcal{C}$-topology on $J(\mathfrak{k}_0)$.

Lemma 27. *For any $f \in \mathcal{C}(\mathfrak{h}_0)$, there exists exactly one element $\psi_f \in I^\infty(\mathfrak{k}_0)$ such that $\pi(H)\psi_f(H) = \sum_{s\in W}\epsilon(s)f(sH)$ $(H \in \mathfrak{h}_0)$. Furthermore, ψ_f lies in $J(\mathfrak{k}_0)$ and $f \to \psi_f$ is a continuous mapping of $\mathcal{C}(\mathfrak{h}_0)$ into $J(\mathfrak{k}_0)$.*

Since $\mathfrak{k}_0 = \bigcup_{k\in K} k\mathfrak{h}_0$, a function in $I^\infty(\mathfrak{k}_0)$ is completely determined by its restriction on $\mathfrak{h}_0'$. Therefore the uniqueness of ψ_f is obvious. Now put $\mathfrak{u} = \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{p}_0$. Then $\mathfrak{u}$ is a compact real form of $\mathfrak{g}$. Let U be the (connected) adjoint group of $\mathfrak{u}$ and let $J(\mathfrak{u})$ denote the set of all functions in $\mathcal{C}(\mathfrak{u})$ which are invariant under U. We consider the $\mathcal{C}$-topology on $J(\mathfrak{u})$. Then from Lemma 17, there exists, for each $f \in \mathcal{C}(\mathfrak{h}_0)$, a unique element $\Psi_f \in J(\mathfrak{u})$ such that

$$\pi(H)\Psi_f(H) = \sum_{s\in W}\epsilon(s)f(sH) \qquad (H \in \mathfrak{h}_0)$$

and $f \to \Psi_f$ is a continuous mapping of $\mathcal{B}(\mathfrak{h}_0)$ into $J(\mathfrak{u})$. Let σ denote the mapping of $\mathcal{B}(\mathfrak{u})$ into $\mathcal{B}(\mathfrak{k}_0)$ which assigns to any function its restriction on $\mathfrak{k}_0$. It is obvious that σ is continuous and it maps $J(\mathfrak{u})$ into $J(\mathfrak{k}_0)$. Therefore $f \to \psi_f = \sigma\Psi_f$ is a continuous mapping of $\mathcal{B}(\mathfrak{h}_0)$ into $J(\mathfrak{k}_0)$ and ψ_f satisfies the condition of the lemma.

Put $I_c^\infty(\mathfrak{k}_0) = I^\infty(\mathfrak{k}_0) \cap C_c^\infty(\mathfrak{k}_0)$, and consider $C_c^\infty(\mathfrak{h}_0)$ and $I_c^\infty(\mathfrak{k}_0)$ under the C_c^∞-topology. If Ω is any compact set in $\mathfrak{h}_0$ and f a function in $C_c^\infty(\mathfrak{h}_0)$ whose carrier lies in Ω, then it is obvious that the carrier of ψ_f is contained in $\Omega' = \bigcup_{k \in K} k\Omega$. Since Ω' is compact, it follows that $\psi_f \in I_c^\infty(\mathfrak{k}_0)$ and $f \to \psi_f$ $(f \in C_c^\infty(\mathfrak{h}_0))$ is a continuous mapping of $C_c^\infty(\mathfrak{h}_0)$ into $I_c^\infty(\mathfrak{k}_0)$.

LEMMA 28. *$D\psi_f = \zeta\psi_{\partial(\bar{\omega})f}$ for all $f \in \mathcal{B}(\mathfrak{h}_0)$.*

It is sufficient to prove that $D\psi_f - \zeta\psi_{\partial(\bar{\omega})f}$ is zero on $\mathfrak{h}_0'$. Select a point $H_0 \in \mathfrak{h}_0'$. We know that $D = \zeta\Delta(\omega)$ on $\mathfrak{k}_0'$, and therefore it follows from the Corollary of Lemma 23 that

$$\psi_f(H_0; D) = \zeta(H_0)\psi_f(H_0; \Delta(\omega)) = \zeta(H_0)\pi(H_0)^{-1}g(H_0; \partial(\bar{\omega})),$$

where g is the function on $\mathfrak{h}_0$ given by

$$g(H) = \pi(H)\psi_f(H) = \sum_{s \in W} \epsilon(s) f^s(H) \qquad (H \in \mathfrak{h}_0).$$

On the other hand, $(\partial(\bar{\omega})f)^s = \partial(\bar{\omega})f^s$ $(s \in W)$ since $\bar{\omega} \in I(\mathfrak{h})$, and therefore $\partial(\bar{\omega})g = \sum_{s \in W} \epsilon(s)(\partial(\bar{\omega})f)^s$. This proves that

$$g(H; \partial(\bar{\omega})) = \pi(H)\psi_{\partial(\bar{\omega})f}(H) \qquad (H \in \mathfrak{h}_0),$$

and therefore $\psi_f(H_0; D) = \zeta(H_0)\psi_{\partial(\bar{\omega})f}(H_0)$.

Let τ be a distribution on $\mathfrak{k}_0$ which is invariant under K. Then we define a distribution Φ on $\mathfrak{h}_0$ by $\Phi(f) = \tau(\zeta\psi_f)$ $(f \in C_c^\infty(\mathfrak{h}_0))$. Notice that if τ is a $\mathcal{B}$-distribution, the same holds for Φ. The following theorem is the main result of this section.

THEOREM 5.[15] *Suppose there exists a complex number c such that $D\tau = c\zeta\tau$. Then Φ coincides with an analytic function on $\mathfrak{h}_0$.*

Let f be a function in $C_c^\infty(\mathfrak{h}_0)$. Then $\tau(D^*\psi_f) = \tau(D\psi_f) = \Phi(\partial(\bar{\omega})f)$ from Lemmas 26 and 28. But $\tau(D^*\psi_f) = c\tau(\zeta\psi_f) = c\Phi(f)$ since $D\tau = c\zeta\tau$. Therefore Φ satisfies the differential equation $\partial(\bar{\omega})\Phi - c\Phi = 0$. But since $\mathfrak{h}_0 \subset \mathfrak{k}_0$, $\bar{\omega}$ is a negative-definite quadratic form on $\mathfrak{h}_0$, and so this equation

[15] Compare this with Theorem 5 of [4(e)].

is of the elliptic type. Hence we can conclude (see [8(I), p. 136] and [5]) that Φ is an analytic function on $\mathfrak{h}_0$.

We shall see in another paper that the above theorem plays an essential role in the theory of Fourier transforms on a noncompact semisimple Lie algebra.

INSTITUTE FOR ADVANCED STUDY,
COLUMBIA UNIVERSITY.

REFERENCES.

[1] P. Cartier, Séminaire "Sophus Lie," 1954-55, Ecole Normale Supérieure, Paris.

[2] C. Chevalley, *Amer. Jour. Math.*, vol. 77 (1955), pp. 778-782.

[3] L. Gårding, *Math. Scand.*, vol. 1 (1953), pp. 55-72.

[4] Harish-Chandra, (a) *Ann. of Math.*, vol. 50 (1949), pp. 900-915.
(b) *Trans. Amer. Math. Soc.*, vol. 70 (1951), pp. 28-96.
(c) " " " " vol. 75 (1953), pp. 185-243.
(d) " " " " vol. 76 (1954), pp. 485-528.
(e) " " " " vol. 83 (1956), pp. 98-163.
(f) *Bull. Amer. Math. Soc.*, vol. 61 (1955), pp. 389-396.
(g) *Amer. Jour. Math.*, vol. 77 (1955), pp. 743-777.
(h) *Proc. Nat. Acad. Sci., U.S.A.*, vol. 42 (1956), pp. 252-253.
(i) " " " " " vol. 42 (1956), pp. 538-540.

[5] F. John, *Proceedings of the symposium on spectral theory and differential problems*, Stillwater, Okla. (1951), pp. 113-175.

[6] J. L. Koszul, *Bull. Soc. Math. France*, vol. 78 (1950), pp. 65-127.

[7] G. D. Mostow, *Bull. Amer. Math. Soc.*, vol. 55 (1949), pp. 969-980.

[8] L. Schwartz, *Théorie des distributions*, I (1950), II (1951), Paris, Hermann.

[9] H. Weyl, *The structure and representations of continuous groups*, Princeton, The Institute for Advanced Study, 1935.

SUR LA CLASSIFICATION DES FIBRES HOLOMORPHES SUR LA SPHERE DE RIEMANN.*

par A. GROTHENDIECK.[1]

Par. 1. Enoncé du théorême principal. Soit X une variété holomorphe (ou plus généralement un "espace analytique" [6]), nous considérons des fibrés holomorphes sur X, de groupe structural un groupe de Lie complexe G. Soit $\boldsymbol{O}_X(G)$ le faisceau des germes d'applications holomorphes de X dans G, (c'est un faisceau de groupes, en général non commutatifs), nous désignerons par $H^1(X, \boldsymbol{O}_X(G))$ l'ensemble des classes de fibrés holomorphes sur X, de groupe structural G. (Pour tout ce qui concerne la notation $H^1(X, \boldsymbol{F})$—où $\boldsymbol{F}$ est un faisceau de groupes non nécessairement commutatifs sur X—et son mécanisme algébrique, voir [4]). Nous n'exigeons pas que G soit connexe, et désignerons par G_0 la composante connexe de l'élément neutre, par $\mathfrak{G}$ son algèbre de Lie. G est dit *réductif* si son algèbre de Lie $\mathfrak{G}$ est réductive, c'est à dire somme directe de son centre et d'une algèbre semi-simple. Par abus de langage, nous appellerons *sous-groupe de Cartan* H de G un sous-groupe holomorphe *connexe* ayant pour algèbre de Lie une sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{G}$. Si G est un groupe algèbrique connexe, cette terminologie coïncide avec elle de [3]. Si Z est le centre de G_0, alors H contient Z_0, et H est l'image réciproque d'un sous-groupe de Cartan H_1 du groupe $G_1 = G_0/Z_0$ (qui est semi-simple dans le cas où G est réductif), D'après la définition générale des sous-algèbres de Cartan [3], si N est le normalisateur de H dans G, le quotient $W = N/H$ est un groupe discret (et même fini si G/G_0 est fini), on l'appelle le *groupe de Weyl* de G.

Tout fibré holomorphe de groupe structural H définissant un fibré holomorphe associé de groupe structural G, on obtient une application canonique $H^1(X, \boldsymbol{O}_X(H)) \to H^1(X, \boldsymbol{O}_X(G))$. D'autre part, N opère par automorphismes intérieurs dans G et H est stable sous ces opérations, d'où d'ensuit que N opère aussi dans les ensembles $H^1(X, \boldsymbol{O}_X(H))$ et $H^1(X, \boldsymbol{O}_X(G))$ et l'application précédente est compatible avec ces opérations. D'ailleurs les opérations sur le deuxième ensemble, correspondant à des automorphismes

* Received October 12, 1956.

[1] La majeure partie de ce travail a été faite en 1955 alors que l'auteur était Visiting Associate Professor à l'Université de Kansas, USA.

intérieurs de G, sont triviales, et pour la même raison les éléments de H opèrent trivialement sur $H^1(X, \boldsymbol{O}_X(H))$, de sorte qu'en fait le groupe de Weyl $W = N/H$ opère sur cet ensemble. On en déduit une application canonique

$$H^1(X, \boldsymbol{O}_X(H))/W \to H^1(X, \boldsymbol{O}_X(G)) \tag{1}$$

où le premier membre désigne l'ensemble des trajectoires dans $H^1(X, \boldsymbol{O}_X(H))$ sous le groupe de Weyl. L'image de cette application est l'ensemble des classes de fibrés holomorphes de groupe G dont le groupe structural peut se réduire au sous-groupe de Cartan H. Le but du présent travail est la démonstration du

THÉORÈME 1.1. *Soit G un groupe de Lie complexe réductif, soit X la sphère de Riemann (c'est à dire une courbe algèbrique complète de genre* 0). *Alors l'application* (1) *est bijective, en d'autres termes: Pour tout fibré holomorphe sur X de groupe structural G, le groupe structural peut se réduire au sous-groupe de Cartan H de G, et ceci de façon unique à une opération du groupe de Weyl W près.*

On peut expliciter ce résultat ainsi. On sait, puisque G est réductif, que H est abélien, soit $\mathfrak{h}$ son algèbre de Lie. L'homomorphisme $h \to \exp. 2i\pi h$ de $\mathfrak{h}$ sur H identifie l'espace vectoriel $\mathfrak{h}$ à un groupe de recouvrement de H, soit P son noyau ("réseau unité" de $\mathfrak{h}$). La suite exacte $0 \to P \to \mathfrak{h} \to H \to 0$ donne une suite exacte de faisceaux abéliens $0 \to P \to \boldsymbol{O}_X(\mathfrak{h}) \to \boldsymbol{O}_X(H) \to 0$ d'où une suite exacte de cohomologie

$$H^1(X, \boldsymbol{O}_X(\mathfrak{h})) \to H^1(X, \boldsymbol{O}_X(H)) \to H^2(X, P) \to H^2(X, \boldsymbol{O}_X(\mathfrak{h})).$$

Or il est bien connu que $H^i(X, \boldsymbol{O}_X) = 0$ pour $i \geqq 1$ ($\boldsymbol{O}_X$ étant le faisceau des germes de fonctions holomorphes sur X) : c'est vrai chaque fois que X est un espace projectif complexe [5]. Par suite on a aussi $H^i(X, \boldsymbol{O}_X(\mathfrak{h})) = 0$, d'où

$$H^1(X, \boldsymbol{O}_X(H)) \approx H^2(X, P) \approx P. \tag{2}$$

Ces isomorphismes sont "fonctoriels," et en particulier compatibles avec les opérations de W, donc on obtient:

COROLLAIRE 1. *Sous les conditions du théorème* 1.1, *l'ensemble $H^1(X, \boldsymbol{O}_X(G))$ s'identifie à l'ensemble P/W, où P est le réseau unité dans l'algèbre de Cartan $\mathfrak{h}$ correspondant au groupe de Cartan H, et W le groupe de Weyl correspondant à H.*

Supposons pour simplifier que G est connexe et semi-simple, considérons

un système fondamental de racines $(\alpha_i)_{1\leq i\leq r}$ sur $\mathfrak{h}$ [2], et la "chambre de Weyl" C formée des $h \in \mathfrak{h}$ tels que $\alpha_i(h) \geqq 0$ pour tout i. On sait que tout élément h de $\mathfrak{h}$ tel que $\alpha_i(h)$ soit réel pour tout i, est conjugué sous W à un élément et un seul de C (savoir le plus grand des transformés de h par W, dans l'ordre lexicographique relatif à une certaine base de $\mathfrak{h}$ [2]). Donc:

COROLLAIRE 2. *Si G est connexe semi-simple, alors $H^1(X, \boldsymbol{O}_X(G))$ s'identifie à l'ensemble des éléments du réseau unité P de G relativement à $\mathfrak{h}$ qui sont dans le chambre de Weyl C.*

En un certain sens, la classification des fibrés holomorphes sur la sphère de Riemann X, de groupe G, est duale de la classification des représentations linéaires de dimension finie de G [2]. On peut préciser ce point en donnant un énoncé équivalent du théorème 1.1 ne faisant plus intervenir de sous-group de Cartan. Pour ceci, rappelons d'abord que le groupe $H^1(X, \boldsymbol{O}_X(\boldsymbol{C}^*))$ des classes de fibrés de groupe $\boldsymbol{C}^*$ [2] sur une variété projective X, s'identifie au groupe des classes de diviseurs sur X mod les diviseurs principaux, donc au group Z des entiers rationnels quand X est la sphère de Riemann. Soit dans ce cas L_1 le fibré vectoriel holomorphe sur X, de fibré $\boldsymbol{C}$ et de groupe $\boldsymbol{C}^*$, correspondant à un diviseur de degré 1. Si G est un groupe de Lie complexe quelconque, et u un homomorphisme complexe de $\boldsymbol{C}$ dans G, on peut considérer le fibré holomorphe de groupe structural G associé à L_1 et à u. La classe de ce fibré ne change évidemment pas si on remplace u par ${}^g u(t) = gu(t)g^{-1}$ (car, comme on l'a déjà remarqué, la permutation de $H^1(X, \boldsymbol{O}_X(G))$ définie par un automorphisme intérieur de G est l'identité). En d'autres termes, désignant par $\mathrm{Hom}(\boldsymbol{C}^*, G)/G$ l'ensemble des classes de homomorphismes complexes de $\boldsymbol{C}^*$ dans G, mod composition avec des automorphismes intérieurs de G, on obtient une application naturelle

$$\mathrm{Hom}(\boldsymbol{C}^*, G)/G \to H^1(X, \boldsymbol{O}_X(G)). \tag{3}$$

THÉORÈME 1.2. *Soit X la sphère de Riemann, G un groupe de Lie complexe réductif. Alors l'application* (3) *est bijective. En d'autres termes, tout fibré holomorphe sur X de groupe G est associé au fibré fondamental L_1 et à un homomorphisme complexe u de $\boldsymbol{C}^*$ dans G, et ce dernier est unique mod. composition avec un automorphisme intérieur de G.*

La démonstration des théorèmes 1.1 et 1.2 sera développée dans les par. 2, 3, 4. Nous allons ici d'abord montrer que le théorème 1.2 est bien

---

[2] C désigne le corps des complexes, C^* le groupe complexe multiplicatif des nombres complexes $\neq 0$.

équivalent au théorème 1.1. Prouvons d'abord que le th. 1.2 est vrai si G est un groupe *abélien connexe* H. Considérons alors le diagramme

$$\begin{tikzcd} \mathrm{Hom}(\boldsymbol{C}^*, H) \arrow[r] & H^1(X, \boldsymbol{O}_X(H)) \\ & P \arrow[ul] \arrow[u] \end{tikzcd}$$

où P est le réseau unité de l'algèbre de Lie $\mathfrak{h}$ de H, où l'homomorphisme horizontal est celui envisagé dans le th. 1.2, et l'homomorphisme vertical droit est l'isomorphisme (2). Le troisième homomorphisme $P \to \mathrm{Hom}(\boldsymbol{C}^*, H)$ est aussi un isomorphisme, obtenu en remarquant que les homomorphismes complexes de $\boldsymbol{C}^* \approx \boldsymbol{C}/\boldsymbol{Z}$ dans $H \approx \mathfrak{h}/P$ correspondent biunivoquement aux homomorphismes de $\boldsymbol{C}$ dans $\mathfrak{h}$ appliquant Z dans P, c'est-à-dire aux éléments de P. Le diagramme ainsi obtenu est commutatif, comme on voit aussitôt, d'où résulte que l'homomorphisme horizontal est lui aussi bijectif.—Passons au cas général où on a un groupe de Lie complexe réductif G quelconque. On a un diagramme commutatif d'applications naturelles:

$$\begin{tikzcd} \mathrm{Hom}(\boldsymbol{C}^*, H)/W \arrow[r, "\alpha'"] \arrow[d, "\beta'"] & \mathrm{Hom}(\boldsymbol{C}^*, G)/G \arrow[d, "\beta"] \\ H^1(X, \boldsymbol{O}_X(H))/W \arrow[r, "\alpha"] & H^1(X, \boldsymbol{O}_X(G)) \end{tikzcd} .$$

Le théorème 1.1 (resp. 1.2) signifie que α (resp. β) est bijectif. Nous venons de voir que $\mathrm{Hom}(\boldsymbol{C}^*, H) \to H^1(X, \boldsymbol{O}_X(H))$ donc aussi β' est bijectif, et nous allons démontrer ci-dessous que α' est aussi bijectif. Il en résulte bien que les théorêmes 1.1 et 1.2 sont équivalents. Il reste donc seulement à prouver l'énoncé suivant, sans doute bien connu, de la théorie des groupes de Lie:

PROPOSITION 1.3. *Soit G un groupe de Lie complexe réductif, H un sous-groupe de Cartan, N le normalisateur de H dans G et $W = N/H$ le groupe de Weyl correspondant. Alors tout homomorphisme complexe de $\boldsymbol{C}^{*n}$ dans G est conjugué par automorphisme intérieur dans G à un homomorphisme complexe de $\boldsymbol{C}^{*n}$ dans H, qui est unique à une opération de W près.*

Pour montrer que tout homomorphisme u de $A = C^{*n}$ dans G est conjugué à un homomorphisme complexe à valeurs dans H, on peut évidemment supposer G connexe (puisque $u(A) \subset G_0$), et ensuite G semi-simple (puisque H est l'image réciproque d'un sous-groupe de Cartan de G/Z_0, où Z est le centre de G). Alors G peut être regardé comme un groupe algébrique linéaire [3]. Comme toute représentation linéaire holomorphe de A est semi-simple

(puisque A est la complexification d'un groupe compact T^n), $u(A)$ est une partie de G formée d'opérateurs semi-simples deux à deux permutables, donc est contenu dans un sous-groupe de Cartan de G [3, Chap. 6, prop. 18], donc, puisque tous les sous-groupes de Cartan de G sont conjugués (loc. cité, th. 4), il existe un $g \in G$ tel que $gu(A)g^{-1} \subset H$, ce qui établit notre assertion. Prouvons maintenant que deux homomorphismes u, u' de A dans H qui sont conjugués dans G, sont conjugués par un élément de N. Il revient au même de dire que si A, B sont deux parties de H et $g \in G$ tels que $gAg^{-1} = B$, alors il existe un $n \in N$ tel que $nan^{-1} = gag^{-1}$ pour tout $a \in A$. (La démonstration très simple qui suit m'a été signalée par A. Borel). Ceci signifie qu'il existe $n \in N$ tel que $m = g^{-1}n$ appartienne au centralisateur M de A. Or $A = g^{-1}Bg$ est contenu dans H et $H' = g^{-1}Hg$, donc M contient H et H', qui sont évidemment encore des sous-groupes de Cartan de M. Il s'ensuit (loc. cité) que l'on peut trouver un $m \in M$ tel que $m^{-1}H'm = H$, et il suffit de poser $n = gm$.

Nous aurons besoin plus bas du résultat suivant, sans doute bien connu; et qui contient prop. 1.3 dans le cas où G est semi-simple connexe:

PROPOSITION 1.4. *Soit G un groupe de Lie complexe connexe semi-simple, H un sous-groupe de Cartan, x et y deux éléments de H tels que pour toute représentation linéaire complexe irreductible de dimension finie U de G, on ait $\operatorname{Tr} U(x) = \operatorname{Tr} U(y)$. Alors x et y sont conjugués sous le groupe de Weyl.*

Donnons la démonstration de ce résultat pour la commodité du lecteur. H est une variété algébrique affine (isomorphe à $\boldsymbol{C}^{*r}$, où r est le rang de G). Soit A l'algèbre des fonctions rationelles sur H, elle s'identifie à l'algèbre du groupe $P^0 \subset \mathfrak{h}'$, réseau du dual $\mathfrak{h}'$ de $\mathfrak{h}$ "polaire" du réseau unité P de $\mathfrak{h}$, à $\lambda \in P^0$ correspondant la fonction $f_\lambda(\exp 2i\pi h) = \exp 2i\pi\langle h, \lambda\rangle$. W est un groupe d'automorphismes de l'algèbre affine A, que peut se définir soit directement à partir des opérations de W sur H, soit par l'intermédiaire des opérations de W sur le groupe P^0. Soit A^W la sous-algèbre des éléments de A invariants sous W, comme W est fini elle "sépare" les trajectoires de W dans H, en d'autres termes deux points x et y de H sont conjugués sous W si et seulement si on a $f(x) = f(y)$ pour toute $f \in A^W$. La proposition sera donc prouvée si nous prouvons que les restrictions à H des caractères des représentations linéaires irréductibles de dimension finie de G engendrent l'espace vectoriel A^W. Or A^W est l'espace vectoriel engendré par les fonctions $\phi_\lambda = \sum_{w \in W} w^*. \ f_\lambda$, où $\lambda \in P^0$. Choisissons une systême fondamental de racines

relatif à H, alors tout élément de P^0 est transformé par W d'un poids dominant d'une représentation linéaire irréductible de G [2], on peut donc se borner à prendre les λ qui sont de tels poids dominants. Or on voit facilement qu'une telle ϕ_λ est bien combination linéaire à coéfficients entiers de caractères de représentations linéaires irréducibles, grâce au fait que dans la représentation linéaire irréductible de poids dominant donné λ, la multiplicité de λ (donc le coéfficient de f_λ dans l'expression du caractère de la représentation envisagée) est 1.

COROLLAIRE. *Soient u, u' deux homomorphismes complexes de $A = \boldsymbol{C}^{*n}$ dans H tels que pour toute représentation linéaire holomorphe irréducible U de dimension finie de G, on ait $\operatorname{Tr} U \circ u = \operatorname{Tr} U \circ u'$. Alors u et u' sont conjuguées par une opération du groupe de Weyl.*

Soit T *la circonférence unité dans* $\boldsymbol{C}^*$, soit t un élément de T^n engendrant un sous-groupe dense, il suffit alors d'appliquer la prop. 1.4 à $u(t)$ et $u'(t)$.

Par. 2. Fibrés vectoriels. Nous allons prouver le théorème 1.1 quand G est le groupe linéaire $\boldsymbol{Gl}(r, \boldsymbol{C})$ des automorphismes de l'espace vectoriel complexe $\boldsymbol{C}^r$. Alors la classification des fibrés holomorphes de groupe $\boldsymbol{Gl}(r, \boldsymbol{C})$ est aussi elle des fibrés vectoriels holomorphes. Notons que le sous-groupe H de $\boldsymbol{Gl}(r, \boldsymbol{C})$ formé des matrices diagonales est un sous-groupe de Cartan. Les fibrés holomorphes vectoriels à groupe structural H s'identifient aux fibrés vectoriels E avec une décomposition donnée $E = \sum_{i=1}^{r} E_i$ de E en somme directe de sous-fibrés vectoriels holomorphes à fibre de dimension 1. Le théorême 1.1 s'énonce maintenant ainsi:

THÉORÈME 2.1. *Soit X la sphère de Riemann. Tout fibré vectoriel holomorphe E sur X est somme directe de sous-fibrés vectoriels holomorphes F_i $(1 \leqq i \leqq r)$ à fibres de dimension 1. Les classes des fibrés F_i sont bien déterminées à une permutation près.*

Si on se rappelle que la classe d'un fibré vectoriel holomorphe à fibre $\boldsymbol{C}^*$ est définie par son degré, qui est un entier rationel arbitraire, on obtient le

COROLLAIRE. *L'ensemble $H^1(X, \boldsymbol{O}_X(\boldsymbol{Gl}(r, \boldsymbol{C})))$ des classes de fibrés vectoriels holomorphes sur la sphère de Riemann X, s'identifie à l'ensemble des suites décroissantes $n_1 \geqq n_2 \geqq \cdots \geqq n_r$ de r entiers rationnels, a une telle suite correspondant la classe du fibré $\sum L_{n_i}$, où L_n est le fibré vectoriel holomorphe de fibre $\boldsymbol{C}$ sur X ayant le degré n.*

La démonstration qui va suivre s'applique aussi bien dans le cadre de la Géométrie Algébrique sur un corps de base algébriquement clos quelconque.

Notons d'abord que d'après Serre [6] la classification des fibrés vectoriels analytiques, ou des fibrés vectoriels algébriques au sens de Weil [8], au dessus d'une variété holomorphe projective (donc algébrique), est la même. Dans le cas où X est une courbe sans singularités, toute application rationelle de X dans une variété projective est régulière (résultat élémentaire purement local) d'où il résulte que plus généralement, toute section rationelle d'un fibré algébrique localement trivial sur X de fibre une variété projective, est en fait régulière. Appliquant ceci au fibré associé au fibré vectoriel algébrique E, de fibré l'espace projectif défini par $\boldsymbol{C}^r$, on voit qu'on peut trouver un sous-fibré vectoriel algébrique E_1 de E à fibre de dimension 1: il suffit de prendre une section rationelle $s \neq 0$ de E, c'est aussi la section rationelle d'un fibré E_1 du type cherché, évidemment unique. (Le fait que E est un fibré *algébrique* nous sert précisément pour assurer l'existence de sections méromorphes non identiquement nulles!). Appliquant ce résultat au fibré vectoriel E/E_1, on construit de proche en proche une "suite de composition" $E_0 = \{0\} \subset E_1 \subset E_2 \subset \cdots \subset E_r = E$ de E par des sous-fibrés vectoriels holomorphes tels que les E_i/E_{i-1} aient des fibres de dimension 1 $(1 \leqq i \leqq r)$. Soit $d_i = d(E_i/E_{i-1})$ le degré de fibré E_i/E_{i-1}, on va pouver que l'on peut choisir la suite de composition de telle sorte que la suite des d_i soit décroissante.

LEMME 2.2. *Les degrés des sous-fibrés vectoriels holomorphes L de E à fibre de dimension 1 sont bornés supérieurement.*

De façon précise, on a $d(L) \leqq \operatorname{Sup}_i d_i$. En effet, soit i le premier indice tel que $L \subset E_i$, soit $s \neq 0$ une section méromorphe de L, s' la section méromorphe de E_i/E_{i-1} qu'elle définit. Les diviseurs de s et s' satisfont évidemment à $(s) \leqq (s')$, d'où $\deg(s) \leqq \deg(s')$ c'est à dire $d(L) \leqq d(L_i)$, cqfd.

Pour construire maintenant les E_i de façon que la suite d_i soit décroissante, prenons d'abord pour E_1 un sous-fibré vectoriel holomorphe de E, de fibré C, de telle façon que $d(E_1)$ soit le plus grand possible, construisons de même le sous-fibré E_2/E_1 de E/E_1, etc. Je dis que la suite des $d_i = d(E_i/E_{i-1})$ est alors décroissante. On est ramené aussitôt à prouver que $d_2 \leqq d_1$, puis en remplaçant E par E_2, au cas où la fibré de E est de dimension 2. On doit donc prouver:

LEMME 2.3. *Soit E un fibré vectoriel holomorphe de fibre C^2 sur la sphère de Riemann X, soit E_1 un sous-fibré vectoriel holomorphe à fibré C, tel que $d(E_1)$ soit le plus grand possible. Alors $d(E_1) \geqq d(E/E_1)$.*

Nous allons prouver en effet que si $d_1 < d_2$, alors il existe un sous-fibré vectoriel holomorphe de E de degré $> d_1$, c'est à dire qu'il existe une section méromorphe $s \neq 0$ de E telle que $\deg(s) > d_1$. Pour ceci, on peut supposer $d_1 = -1$ d'où $d_2 \geqq 0$, en remplaçant au besoin E par son produit tensoriel avec un fibré vectoriel holomorphe L_{-1-d_1} de degré $-1-d_1$. (En effet, les sous-fibrés vectoriels holomorphes de E et de $L \otimes E$ sont en correspondance biunivoque par $E_1 \to L \otimes E_1$, et $L \otimes E/E_1$ est isomorphe à $(L \otimes E)/(L \otimes E_1)$, enfin le degré de $L \otimes E_1$ resp. $L \otimes E/E_1$ est égal à celui de E_1 resp. E/E_1 augmenté de $n = -1-d_1$). Pour un fibré vectoriel holomorphe M quelconque, désignons par $\boldsymbol{O}_X(M)$ le faiseau des germes de sections holomorphes de M. On a alors une suite exacte de faisceaux $0 \to \boldsymbol{O}_X(E_1) \to \boldsymbol{O}_X(E) \to \boldsymbol{O}_X(E/E_1) \to 0$, d'où une suite exacte de cohomologie

$$H^0(X, \boldsymbol{O}_X(E)) \to H^0(X, \boldsymbol{O}_X(E/E_1)) \to H^1(X, \boldsymbol{O}_X(E_1)).$$

Or d'après le théorème de dualité [7], $H^1(X, \boldsymbol{O}_X(E_1))$ a même dimension que $H^0(X, \boldsymbol{O}_X(L_{k-d_1}))$ où $k = 2g-2$ est le degré de la "classe canonique" de diviseurs (g désigne le genre de X). Or on a $g = 0$, $d_1 = -1$, d'où $L_{k-d} = L_{-1}$; le diviseur d'une section méromorphe de L_{-1} a pour degré -1, donc ne peut être $\geqq 0$, donc $H^0(X, \boldsymbol{O}_X(L_{-1})) = 0$ et par suite $H^1(X, \boldsymbol{O}_X(E_1)) = 0$, donc la suite exacte précédente prouve que toute section holomorphe de E/E_1 provient d'une section holomorphe de E. Or, comme E/E_1 a un degré $d_2 \geqq 0$, il admet une section holomorphe non nulle, il en est donc de même de E. Une section holomorphe non nulle s de E a un diviseur de degré $\geqq 0$ donc de degré $> d_1 = -1$, ce qui achéve la démonstration du lemme 2.3.[3]

Soit donc (E_i) une suite de composition du fibré vectoriel E, telle que la suite des degrés d_i des E_i/E_{i-1} $(1 \leqq i \leqq r)$ soit décroissante, nous allons prouver que E est isomorphe à la somme directe des E_i/E_{i-1}. On procède par récurrence sur r, l'assertion étant triviale pour $r = 1$. Supposons la démontrée pour des fibrés vectoriels de fibre $\boldsymbol{C}^{r'}$ avec $r' \leqq r-1$ (r étant un entier $\geqq 2$), prouvons la pour E de fibre $\boldsymbol{C}^r$. D'après l'hypothèse de récurrence, E_{r-1} est isomorphe à $\sum_{i=1}^{r-1} E_i/E_{i-1}$, nous allons prouver que l'extension E du fibré vectoriel $Q = E/E_{r-1}$ par le fibré vectoriel $P = E_{r-1}$ est triviale, c'est à dire qu'il existe un homomorphisme holomorphe de Q dans E qui, composé avec l'homomorphisme canonique $E \to Q$, donne l'identité. Soit Q'

[3] Cette démonstration est due à J. P. Serre. La démonstration originale était beaucoup moins transparente.—Le referee fait remarquer que ce résultat figure aussi, sous une forme différente, dans Atiyah, Proc. L. M. S. 1955.

le fibré dual de Q. La suite exacte $0 \to Q' \otimes P \to Q' \otimes E \to Q' \otimes Q \to 0$ donne naissance à une suite exacte de cohomologie

$$H^0(X, \boldsymbol{O}_X(Q' \otimes E)) \to H^0(X, \boldsymbol{O}_X(Q' \otimes Q)) \to H^1(X, \boldsymbol{O}_X(Q' \otimes P)).$$

Or on a

$$Q' \otimes P \approx \sum_{i=1}^{r-1} (E/E_{r-1})' \otimes (E_i/E_{i-1}) \approx \sum_{i=1}^{r-1} L_{d_i - d_r}$$

d'où $H^1(X, \boldsymbol{O}_X(Q' \otimes P)) \approx \sum_{i=1}^{r-1} H^1(X, \boldsymbol{O}_X(L_{d_i - d_r}))$, et comme $d_i - d_r \geqq 0 > -1$, un calcul déjà fait montre que $H^1(X, \boldsymbol{O}_X(L_{d_i - d_r})) = 0$, d'où $H^1(X, \boldsymbol{O}_X(Q' \otimes P)) = 0$. Donc le premier homomorphisme de la suite exacte écrite plus haut est surjectif, en particulier l'automorphisme identique de Q (considéré comme section holomorphe du fibré $Q' \otimes Q$) appartient à cette image, i.e., peut se remonter en un homomorphisme holomorphe de Q dans E.[4]

On a démontré la première partie du théorème 2.1. Reste à prouver que dans une décomposition en somme directe $E = \sum F_i$, les degrés des fibrés F_i de fibré C sont bien déterminés à l'ordre près. Ce fait pourrait se déduire d'un théorème du type Remak-Krull, dû à Atiyah (non publié), affirmant que la décomposition d'un fibré vectoriel holomorphe, sur un espace analytique compact X, en somme directe de fibrés vectoriels "indécomposables," est essentiellement unique. Mais nous aurons besoin dans le cas actuel d'un résultat plus précis, que voici:

Proposition 2.4. *Soit* $E = \sum_{i=1}^{r} F_i$ *un fibré vectoriel holomorphe sur la sphère de Riemann X, somme directe de sous-fibrés vectoriels holomorphes à fibré* $\boldsymbol{C}$, *de degrés* d_i. *Soit, pour tout entier rationnel k, E_k le sous-fibré vectoriel de E, somme directe des F_i tels que $d_i \geqq k$. Alors E_k est égal au plus petit sous-fibré vectoriel holomorphe de E contenant les sections méromorphes s de E dont le diviseur est de degré $\geqq k$ (en particulier, E_k est défini indépendamment de la décomposition donnée de E).*

Corollaire. *Le nombre d'indices i tels que $d_i = k$ est égal à la dimension de la fibre du fibré vectoriel E_k/E_{k+1}, donc ne dépend pas de la décomposition choisie de E.*

La démonstration de la proposition 2.4 est immédiate, et laissée au lecteur.

---

[4] Nous avons montré que si P et Q sont deux fibrés vectoriels holomorphes sur l'espace analytique X, tels que $H^1(X, \boldsymbol{O}_X(Q' \otimes P)) = 0$, alors toute extension holomorphe de Q par P est triviale. En fait, il n'est pas difficile de se convaincre que dans tous les cas, les classes d'extensions holomorphes de Q par P correspondent biunivoquement aux éléments de $H^1(X, \boldsymbol{O}_X(Q' \otimes P))$ (Serre).

Par. 3. Fibrés orthogonaux.

PROPOSITION 3.1. *Soit X un espace analytique compact. L'application canonique de $H^1(X, \boldsymbol{O}_X(\boldsymbol{O}(r, C)))$ dans $H^1(X, \boldsymbol{O}_X(\boldsymbol{Gl}(r, \boldsymbol{C})))$ déduite de l'injection naturelle $\boldsymbol{O}(r, \boldsymbol{C}) \rightarrow \boldsymbol{Gl}(r, C)$ est injective.*

En d'autres termes, deux fibrés vectoriels orthogonaux holomorphes sur X, isomorphes en tant que fibrés vectoriels holomorphes, sont aussi isomorphes en tant que fibrés vectoriels orthogonaux holomorphes. Pour le prouver, on peut supposer que sur le fibré vectoriel holomorphe E, on a deux structures orthogonales holomorphes définies par la donnée sur toute fibre E_x $(x \in X)$ de deux formes quadratiques (a, b) et $(a, b)_1$ non dégénérées, (fonctions holomorphes du point x), et il faut montrer qu'il existe un automorphisme holomorphe u du fibré vectoriel E, transformant la première forme en la seconde, c'est à dire tel que $(a, b)_1 = (ua, ub)$ pour $a, b \in E_x$. Pour toute fibre E_x, on peut écrire $(a, b)_1 = (A_x a, b)$, où A_x est un endomorphisme de E_x tel que $A = A^*$ (où A^* est l'adjoint de A relativement à la première forme quadratique: $(A^*a, b) = (a, Ab)$ pour $a, b \in E_x$). A_x est inversible, et pour x variable, est une fonction holomorphe de x, donc définit un automorphisme A du fibré vectoriel E. On cherche donc un automorphisme vectoriel holomorphe u de E tel que $(ua, ub) = (Aa, b)$ c'est à dires $A = u^*u$. On va voir qu'on peut même choisir u tel $u = u^*$, et $A = u^*u = u^2$. Pour ceci, considérons le polynôme caractéristique $\det(A - z \cdot 1)$ de A, ses coéfficients sont des fonctions holomorphes sur X, donc constantes puisque X est compacte, pourvu qu'on suppose X connexe, ce qui est loisible. Donc le polynôme caractéristique de A_x est indépendant de x. Soient $\lambda_1, \cdots, \lambda_k$ ses racines distinctes, de multiplicités $\alpha_1, \cdots, \alpha_k$. Pour tout $x \in X$, E_x est somme directe de sous-espaces E^i_x bien déterminés, de dimension α_i, sur chacun desquels A_x induit un opérateur de la form $\lambda_i(\mathbf{1} + u^i_x)$, où u^i_x est nilpotent. Les E^i_x sont orthogonaux deux à deux puisque $A = A^*$. Les E^i_x et les u^i_x sont fonction holomorphes de x, donc E est somme directe de sous-fibrés vectoriels holomorphes E^i $(1 \leqq i \leqq k)$, tels que la fibre de E^i en x soit E^i_x. Soit μ_i une racine carrée de λ_i, posons

$$v^i_x = \mu_i(\mathbf{1} + u^i_x)^{\frac{1}{2}}$$

où on pose $(\mathbf{1} + u^i_x)^{\frac{1}{2}} = \sum_{k=0}^{\alpha_i - 1} (1/k!)\left(\tfrac{1}{2}\right)\left(\tfrac{1}{2} - 1\right) \cdots \left(\tfrac{1}{2} - k + 1\right)(u^i_x)^k$. Alors v^i_x est un endomorphisme de E^i_x fonction holomorphe de x, de plus on a $v^i_x = (v^i_x)^*$. Soit v^i l'endomorphisme de E^i défini par les v^i_x, u leur somme directe, on a $u = u^*$ puisque les v^i sont autoadjoint et les E^i orthogonaux

deux à deux, et de plus $u^2 = A$ par construction, ce qui achève la démonstration.

Remarques 1. La démonstration qui précède est encore valable en Géométrie Algébrique sur un corps algébriquement clos quelconque de caractéristique $p \neq 2$. Une démonstration exactement analogue prouverait de même que l'application canonique

$$H^1(X, \boldsymbol{O}_X(\boldsymbol{Sp}(r, \boldsymbol{C}))) \to H^1(X, \boldsymbol{O}_X(\boldsymbol{Gl}(2r, \boldsymbol{C})))$$

est injective sous les mêmes conditions. On pourrait en déduire directement, comme pour le cas du groupe structural $\boldsymbol{O}(r, \boldsymbol{C})$ traité ci-dessous, la classification des fibrés symplectiques holomorphes sur la sphère de Riemann. Cette démonstration a l'avantage d'être encore directement applicable en Géométrie Algébrique (en caractéristique $p \neq 2$), contrairement à celle du par. 4.

2. L'analogue de la Proposition 3.1 pour le groupe structural $\boldsymbol{SO}(r, \boldsymbol{C})$ au lieu de $\boldsymbol{O}(r, \boldsymbol{C})$ est fausse déjà si $r = 2$ et quand X est la sphère de Riemann.

En vertu de prop. 3.1, la détermination de $H^1(X, \boldsymbol{O}_X(\boldsymbol{O}(r, \boldsymbol{C})))$ revient à la détermination de l'image de cet ensemble dans $H^1(X, \boldsymbol{O}_X(\boldsymbol{Gl}(r, \boldsymbol{C})))$. On a alors:

THÉORÈME 3.2. *Soient X la sphère de Riemann, E un fibré vectoriel holomorphe sur X. Pour qu'il existe sur E une structure orthogonale holomorphe, il faut et il suffit que E soit isomorphe au fibré dual E'. Alors le fibré orthogonal dont il provient est bien déterminé à un isomorphisme près.*

La nécessité de la condition est triviale, et le résultat d'unicité est un cas particulier de prop. 3.1. Reste à prouver que si E est isomorphe à E', E admet une structure orthogonale holomorphe. Mais soit (n_i) la suite des invariants de E (th. 2.1, corollaire) alors la suite des invariants de E' est évidemment à l'ordre près $(-n_i)$, et l'hypothèse signifie que ces deux suites sont les mêmes à une permutation près, c'est à dire que la famille (n_i) est symétrique par rapport à 0. Dans la décomposition $E \approx \sum L_{n_i}$ on peut donc grouper ensemble les composantes qui correspondent à des n_i nuls, et les E_i correspondants à des n_i opposés, donc E apparait comme somme directe d'un fibré trivial E_0, et de fibrés du type $L + L'$. E_0 peut évidemment se munir d'une structure orthogonale, donc le théorème résultera du

LEMME 3.3. *Soit L un fibré vectoriel holomorphe sur un espace ana-*

lytique X, soit L' son dual. Alors le fibré $L+L'$ est muni d'une structure orthogonale canonique.

Il suffit en effet, sur chaque fibré $L_x+L'_x$, d'introduire la forme bilinéaire symétrique

$$(a+a', b+b') = \langle a, b'\rangle + \langle b, a'\rangle$$

où les produits scalaires du second membres sont relatifs à l'accouplement naturel de L_x et de son dual.

PROPOSITION 3.4. *Soient X la sphère de Riemann, E un fibré vectoriel orthogonal sur X, et soit pour tout entier rationnel k, E_k le plus petit sous-fibré vectoriel holomorphe de E contenant les sections méromorphes ayant un diviseur de degré $\geqq k$ (cf. prop. 2.4). Alors le sous-fibré vectoriel de E orthogonal de E_k est E_{-k+1}.*

Par raison de symétrie, on peut supposer $k\geqq 1$. D'après le théorème 3.2, E est de la forme

$$E = E_0 + \sum_{n_i>0} (L_{n_i} + L_{-n_i})$$

où les facteurs E_0 et $(L_{n_i}+L_{-n_i})$ sont deux à deux orthogonaux, enfin les L_{n_i} et L_{-n_i} isotropes et E_0 constant. La proposition résults alors immédiatement de la prop. 2.4.

Par. 4. Démonstration du théorème principal. a) *Reduction du group structural.*

LEMME 4.1. *Soient X un espace analytique complexe compact, G un groupe de Lie complexe, P un fibré holomorphe sur X de groupe structural G, E le fibré associé adjoint de fibre l'algèbre de Lie $\mathfrak{G}$ de G (où G opère par la représentation adjointe). Supposons qu'on connaisse une section holomorphe s de E telle que, en au moins un point $a\in X$, $s(a)$ soit un élément régulier* [3, Chap. 6] *de l'algèbre de Lie E_a, fibre de E en a. Alors $s(x)$ est un élément régulier de E_x pour tout $x\in X$.*

Les coéfficients $a_i(s(x))$ du polynôme caractéristique de $\operatorname{ad} s(x)$ sont des fonctions holomorphes sur X, donc constantes puisque X est compact. Or dire que $s(x)$ est régulier signifie que $a_r(s(x))\neq 0$, où r est le rang de $\mathfrak{G}$. D'où la conclusion.

COROLLAIRE 1. *Sous les conditions précédentes, on peut réduire le groupe structural G de P au normalisateur N d'un sous-groupe de Cartan H de G.*

En effet, soit pour tout $x \in X$, $\mathfrak{h}(x)$ la sous-algèbre de E_x centralisateur de $s(x)$. C'est une sous-algèbre de Cartan puisque x est régulier, et elle est fonction holomorphe de x comme on le vérifie sans difficulté. Soit $\mathfrak{h}$ une sous-algèbre de Cartan de $\mathfrak{G}$, H le sous-groupe de Cartan correspondent de G. Le normalisateur N de H est aussi identique à l'ensemble des $g \in G$ qui invarient $\mathfrak{h}$ dans la représentation adjointe de G. Donc l'espace homogène G/N est isomorphe à l'espace des sous-algèbres de Cartan de $\mathfrak{G}$ (se rappeler que deux sous-algèbres de Cartan sont toujours conjugées!) et le fibré associé à P et de fibre G/N est celui dont la fibre, en un point $x \in X$, est l'ensemble des sous-algèbres de Cartan de l'algèbre de Lie E_x. Or nous avons construit une section holomorphe $x \to \mathfrak{h}(x)$ de ce fibré, ou ce qui revient au même, nous avons réduit à N le groupe structural de P, ce qui prouve le corollaire.

COROLLAIRE 2. *Si de plus X est simplement connexe, on peut réduire le groupe structural au sous-groupe de Cartan H.*

En effet, N/H est discret, donc le fibré de fibre N/H associé à un fibré holomorphe de groupe N est trivial puisque X est simplement connexe, donc le groupe structural peut se réduire à H.

Nous supposons maintenant que X est la sphère de Riemann, et allons montrer que si G est un groupe de Lie holomorphe *réductif*, la condition du lemme 4.1 est automatique satisfaite, c'est à dire qu'on peut trouver une section holomorphe s de E telle que $s(a)$ soit un élément régulier de E_a pour au moins un $a \in X$. On a $\mathfrak{G} = \mathfrak{Z} + \mathfrak{G}'$ où $\mathfrak{Z}$ est le centre et $\mathfrak{G}'$ l'algèbre dérivée de $\mathfrak{G}$, et cette décomposition est invariante sous la représentation adjointe de G. Il en résulte une décomposition analogue de E en somme directe de deux sous-fibrés dont la fibre en chaque point x est le centre resp. l'algèbre dérivée de l'algèbre E_x. Comme un élément régulier de l'algèbre dérivée de E_x est régulier dans E_x, on voit aussitôt, en envisageant le fibré de fibre $\mathfrak{G}'$, de groupe Aut $\mathfrak{G}'$ associé au fibré P et à la représentation de G dans Aut $\mathfrak{G}'$ déduite de la représentation adjointe, qu'on peut se ramener au cas où G est un groupe semi-simple (savoir Aut $\mathfrak{G}'$), ce que nous supposerons désormais.

Soit alors E_k le sous-fibré vectoriel de E engendré par les sections méromorphes dont le diviseur est de degré $\geqq k$ (cf. prop. 2.4). On vérifie aussitôt que $[E_k, E_{k'}] \subset E_{k+k'}$ car si s, s' sont deux sections méromorphes de E, le degré $\deg([s, s'])$ du diviseur de la section $[s(t), s'(t)]$ est manifestement $\geqq \deg(s) + \deg(s')$, car $([s, s']) \geqq (s) + (s')$. Il en resulte en particulier que E_1 est un fibré de *sous-algèbres* de Lie de E, et que si $\mathfrak{G}_1$ est la fibre de E_1 en un point fixé $a \in X$, et si on identifie $\mathfrak{G}$ à la fibre E_a.

alors pour $Y \in \mathfrak{G}_1$, $\operatorname{ad}_{\mathfrak{G}} Y$ est *nilpotent*. D'autre part, E est en fait un fibré orthogonal (grâce à la forme de Killing sur $\mathfrak{G}$, invariante par automorphismes) et nous avons vu (corollaire au th. 3.2) que l'orthogonal de E_1 est forcément E_0. Soit $\mathfrak{G}_0$ la fibre de E_0 en a, c'est donc l'orthogonal de $\mathfrak{G}_1$ dans $\mathfrak{G}$ pour la forme de Killing. Or on a:

LEMME 4.2. *Soient $\mathfrak{G}$ une algèbre de Lie complexe semi-simple, $\mathfrak{G}_1$ une sous-algèbre telle que pour tout $X \in \mathfrak{G}_1$, $\operatorname{ad}_{\mathfrak{G}} X$ soit nilpotent. Par suite $\mathfrak{G}_1$ est nilpotent et à fortiori contenue dans une sous-algèbre résoluble maximale $\mathfrak{R}$ de $\mathfrak{G}$. Alors $\mathfrak{R}$ est contenue dans l'orthogonal $\mathfrak{G}_0$ de $\mathfrak{G}_1$ (pour la forme de Killing).*

En effet, on sait qu'on a $\mathfrak{R} = \mathfrak{h} + \mathfrak{N}$, où $\mathfrak{h}$ est une sous-algèbre de Cartan, et $\mathfrak{N} = \mathfrak{R}'$ est le plus grand idéal nilpotent de $\mathfrak{R}$. Il s'ensuit que tout élément X de $\mathfrak{R}$ tel que $\operatorname{ad}_{\mathfrak{G}} X$ soit nilpotent est dans $\mathfrak{N}$ (il suffit même que $\operatorname{ad}_{\mathfrak{R}} X$ soit nilpotent!) en particulier $\mathfrak{G}_1 \subset \mathfrak{N}$. D'autre part, il est bien connu aussi que $\mathfrak{R}$ est orthogonal à $\mathfrak{N}$, donc à fortiori à $\mathfrak{G}_1$, donc contenu dans $\mathfrak{G}_0$. Le lemme 4.2 est démontré. Comme il existe des éléments réguliers dans $\mathfrak{h}$, on obtient le

COROLLAIRE. *Sous les conditions précédentes, il existe un élément régulier de $\mathfrak{G}$ contenu dans $\mathfrak{G}_0$.*

Revenons alors à notre démonstration. D'après sa définition et prop. 2.4, E_0 est isomorphe à une somme directe de fibrés vectoriels holomorphes de fibre $\boldsymbol{C}$, de degrés $\geqq 0$, d'où résulte aussitôt que pour tout élément u de la fibré $\mathfrak{G}_0$ de E_0 en a, il existe une section holomorphe s de E_0 prenant la valeur u en a. D'après le corollaire précédent, on peut choisir u régulier. Cela prouve que la condition du lemme 4.1 est bien satisfaite. En vertu du corollaire 2 dudit lemme, nous voyons que le groupe structural de P peut se réduire à H, ce qui démontre la première moitié du théorème principal 1.1: l'application (1) du par. 1 est surjective. Reste à prouver qu'elle est injective.

b) *Résultat d'unicité à une opération de W près.* Dans ce qui suit, X sera toujours la sphère de Riemann. Supposons d'abord G semi-simple connexe. Soit ξ un élément de $H^1(X, \boldsymbol{O}_X(H))$, ξ_1 son image dans $H^1(X, \boldsymbol{O}_X(G))$. On a vu au par. 1 que ξ est la classe du fibré associé au fibré L_1 (de groupe $\boldsymbol{C}^*$) et à un homomorphisme complexe u de $\boldsymbol{C}^*$ dans H bien déterminé. Nous allons montrer comment la connaissance de ξ_1 déter-

mine u à une opération de W près. Pour toute représentation linéaire complexe de G, on a une application naturelle

$$H^1(X, \boldsymbol{O}_X(G)) \xrightarrow{u^*} H^1(X, \boldsymbol{O}_X(\boldsymbol{Gl}(r, \boldsymbol{C})))$$

(r étant le degré de la représentation), en faisant correspondre à un fibré holomorphe de groupe G le fibré vectoriel associé (pour la représentation U). Ce dernier est aussi associé à L_1 et la représentation linéaire $U \circ u$ de $\boldsymbol{C}^*$, donc la classe du fibré vectoriel associé à L_1 et $U \circ u$ est connue quand on connait ξ_1. D'après le théorème 1, 2, déjà démontré (sous la forme équivalente 1. 1) au par. 2 dans le cas du groupe linéaire général, on en conclut que $U \circ u$ est connu à une similitude près, à fortiori la fonction $\mathrm{Tr}\, U(u(t))$ sur $\boldsymbol{C}^*$ est connue. Ceci étant vrai pour toute représentation linéaire U de dimension finie de G, on peut en conclure, en vertu de prop. 1. 4, corollaire, que u lui-même est déterminé à une opération de W près.

Supposons maintenant G réductif et connexe.

LEMME 4. 3. *Soit G un groupe de Lie complexe réductif connexe. Alors il existe un sous-groupe fini z du centre de G tel que G/z soit isomorphe au produit d'un groupe abélien par un groupe semi-simple.*

Le groupe de revêtement universel de G est isomorphe à un produit $V \times F$, où V est un espace vectoriel complexe et F un groupe semi-simple complexe. G est donc isomorphe au quotient de $V \times F$ par un sous groupe discret Γ du centre de $V \times F$. Ce centre est identique à $V \times \pi$, où π est le centre de F, donc fini en vertu d'un théorème fondamental de H. Weyl [2]. Il en résulte que la projection L de Γ sur V est un sous-groupe *fermé* de V, de *même rang* que Γ, donc Γ est un sous-groupe d'indice fini de $L \times \pi$. Posant maintenant $z = (L \times \pi)/\Gamma$, le lemme 4. 3 est démontré.

Le théorème 1. 1 étant vrai si G est semi-simple connexe comme on a vu plus haut, ou si G est abélien connexe comme on a vu au par. 1, il s'ensuit aussitôt qu'il est encore vrai pour le produit de deux tels groupes, donc pour le group G/z du lemme 4. 3. Notons que H/z est un sous-groupe de Cartan de G/z et N/z son normalisateur. Considérons le diagramme commutatif d'applications naturelles:

$$\begin{array}{ccc} H^1(X, \boldsymbol{O}_X(H)) & \longrightarrow & H^1(X, \boldsymbol{O}_X(G)) \\ \downarrow & & \downarrow \\ H^1(X, \boldsymbol{O}_X(H/z)) & \longrightarrow & H^1(X, \boldsymbol{O}_X(G/z)). \end{array}$$

Soient ξ, ξ' deux éléments de $H^1(X, \boldsymbol{O}_X(H))$ ayant même image dans

$H^1(X, \boldsymbol{O}_X(G))$, alors leurs images ξ_1, ξ'_1 dans $H^1(X, \boldsymbol{O}_X(H/z))$ ont même image dans $H^1(X, \boldsymbol{O}_X(G/z))$, donc d'après ce qu'on a dit, sont conjugués sous le groupe de Weyl $(N/z)/(H/z)$ de G/z, qui est isomorphe au groupes de Weyl $W = N/H$ de G. Par suite ξ et ξ' sont conjugués sous W mod un élément du noyau de l'homomorphisme $H^1(X, \boldsymbol{O}_X(H)) \to H^1(X, \boldsymbol{O}_X(H/z))$. Or ce noyau est nul, en vertu de la suite exacte de cohomologie déduite de la suite exacte $0 \to z \to H \to H/z \to 0$, puisque $H^1(X, z) = 0$ (X étant simplement connexe). Cela démontre le th. 1.1 dans le cas où G est connexe.

Supposons enfin G réductif quelconque. Soient ξ, ξ' deux éléments de $H^1(X, \boldsymbol{O}_X(H))$ ayant même image dans $H^1(X, \boldsymbol{O}_X(G))$. Soient ξ_1, ξ'_1 leurs images dans $H^1(X, \boldsymbol{O}_X(G_0))$, ξ_1 et ξ'_1 ont même image dans $H^1(X, \boldsymbol{O}_X(G))$, et sont par suite conjugués par une opération du groupe $H^0(X, \boldsymbol{O}_X(G/G_0)) = G/G_0$ (en vertu par exemple de la "suite exacte de cohomologie" pour les faisceaux non commutatifs, développée dans [4]). Un élément de G/G_0 opère sur $H^1(X, \boldsymbol{O}_X(G_0))$ en prenant un représentant $g \in G$ et considérant l'automorphisme $g_0 \to g g_0 g^{-1}$ de G_0. Or il existe un représentant qui est dans N, comme on a vu à la fin de la démonstration de prop. 1.3. On en conclut qu'en remplaçant ξ' par un conjugué de ξ' sous W, on peut supposer que $\xi_1 = \xi'_1$. D'après le théorème 1.1 pour G_0, on en conclut que ξ et ξ' sont conjugués sous le groupe de Weyl de G_0 et à fortiori sous W, ce qui achève la démonstration.

Remarques finales. 1. On peut se demander si le th. 1.1 ou le th. 1.2 reste valable pour *tout* groupe structural de Lie complexe G. On s'aperçoit qu'il est déjà en défaut quand G est le groupe des transformations affines $z \to az + b$ (a, b complexes). On notera cependant que la technique de "dévissage" exposée dans [4], jointe aux résultats de ce travail, permettent en principe de déterminer $H^1(X, \boldsymbol{O}_X(G))$ pour tout groupe G donné. Je ne connais toutesfois pas de description simple de $H^1(X, \boldsymbol{O}_X(G))$ en termes de théorie des groupes de Lie complexes.

2. Il semble plausible que la seule variété projective X sur laquelle tout fibré vectoriel holomorphe soit décomposable en somme de fibrés holomorphes de fibre $\boldsymbol{C}$, soit la sphère de Riemann. On note en tous cas que si X est une courbe algébrique projective non singulière de genre $g \neq 0$, i.e. telle que $H^1(X, \boldsymbol{O}_X) \neq 0$, il existe sur X un fibré vectoriel holomorphe *indécomposable* à fibre $\boldsymbol{C}^2$: si E_0 est le fibré vectoriel constant de fibre $\boldsymbol{C}$, il suffit de prendre un fibré E extension non triviale[4] de E_0 par E_0. E est indécomposable, car s'il était décomposé en la somme de deux fibrés E_1, E_2

de fibre C, on conclurait d'abord que chaque E_i admet une section holomorphe non nulle (puisque E en admet une engendrant un sous-fibré qui n'est pas "facteur direct") donc a un degré $\geqq 0$; comme la somme de ses degrés est identique à $\deg(E) = \deg(E_0) + \deg(E_0) = 0$, ils doivent être nuls, ce qui, joint à l'existence d'un section holomorphe, implique que E_i est constant, donc E est constant; mais alors toute section holomorphe de E est constante, donc si elle est $\neq 0$, la structure d'extension qu'elle définit sur E est triviale, contrairement à la construction de E comme extension non triviale. Notons encore que si X est l'espace projectif complexe P^n de dimension $n \geqq 2$, alors le fibré tangent n'est pas même réductible à la forme triangulaire; autrement, le fibré dual E le serait aussi, d'où on conclurait aisément que $H^i(X, \boldsymbol{O}_X(E)) = 0$ pour $i \neq 0, n$ (car on sait que pour tout fibré vectoriel holomorphe L de fibré $\boldsymbol{C}$ sur $X = P^n$, on a $H^i(X, \boldsymbol{O}_X(L)) = 0$ si $i \neq 0, n$ [5, Chap. 3, prop. 8]); or $\boldsymbol{O}_X(E)$ est le faisceau Ω^1 des germes de 1-formes différentielles holomorphes, et $H^1(X, \Omega^1) = H^{1,1}(X, \boldsymbol{C})$ (cohomologie de type (1, 1) de X); mais il est bien connu que $H^{1,1}(X, \boldsymbol{C}) \neq 0$ pour toute variété projective sans singularités X de dimension complexe $\geqq 1$. Pour finir, prenons pour X la "variété des drapeaux" sur P^2 (isomorphe canoniquement à la variété des drapeaux dans l'espace vectoriel $\boldsymbol{C}^3$), c'est donc un espace fibré algébrique sur P^2 de fibre P^1 = sphère de Riemann. Le fibré tangent de la base P^2 n'est pas réductible à la forme triangulaire, mais son image réciproque E sur X l'est évidemment, E est cependant, indécomposable, comme il résulte du fait plus général suivant: Soit p une application holomorphe d'un espace analytique X sur un autre Y, identifiant Y à un "espace analytique quotient" de X, i.e. telle que les fonctions holomorphes f sur un ouvert U de Y soient celles telles que $f \circ p$ soit holomorphe sur $p^{-1}(U)$. Supposons que pour tout $y \in Y$, $p^{-1}(y)$ soit compact et connexe. Soit E un fibré vectoriel holomorphe sur Y; *pour que E soit indécomposable, il faut et il suffit que $p^{-1}(E)$ le soit.* De façon plus précise, les décompositions de E en somme directe de deux sous-fibrés vectoriels holomorphes correspondent biunivoquement aux decompositions analogues de $p^{-1}(E)$. Elles s'identifient en effet aux systêmes de deux projecteurs complémentaires de l'algèbre $H^0(Y, \boldsymbol{O}_Y(E' \otimes E))$ (E' désignant le fibré dual de E), tandis que les décompositions de $p^{-1}(E)$ s'identifient aux systêmes de deux projecteurs complémentaires dans l'algèbre $H^0(X, \boldsymbol{O}_X(p^{-1}(E' \otimes \mathrm{E})))$, et il suffit de montrer que si (f_1, f_2) est un tel systême, alors chaque section f_i provient d'une section holomorphe de $E' \otimes E$ sur Y, ou encore (en vertu de l'hypothèse sur p) que sa restriction aux "fibres" $p^{-1}(y)$ sont des sections *constantes*. Or, ceci

résulte du fait que $p^{-1}(E' \otimes E)$ induit un fibré constant sur chaque fibre, et de l'hypothèse faite sur les fibres.[5]

UNIVERSITY OF KANSAS AND
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE.

REFERENCES.

[1] H. Cartan, *Séminaire E. N. S.*, 1953-1954.

[2] P. Cartier, *Séminaire Sophus Lie*, 1. ère année (1954-1955).

[3] C. Chevalley, *Théorie des Groupes de Lie III*, Paris (1955).

[4] A. Grothendieck, *A General Theory of Fibre Spaces with Structure Sheaf*, University of Kansas (1955).

[5] J. P. Serre, "Faisceaux Algébriques Cohérents," *Annals of Mathematics*, vol. 61 (1955), pp. 197-278.

[6] ———, Géometrie Algébrique et Géométrie Analytique, Annales de l'Inst. Fourier, vol. 6 (1955-56), pp. 1-42.

[7] ———, "Un Théorême de Dualité," *Comm. Math. Helvet.*, vol. 29 (1955), pp. 9-26.

[8] A. Weil, *Fibre Spaces in Algebraic Geometry* (Notes by A. Wallace), Chicago University, 1952.

[5] Comme me l'a fait observer le referee, la condition que la fibre soit connexe (et que j'avais malencontreusement omise) est essentielle pour la validaté du résultat indiqué, un contre-exemple dans le cas contraire étant obtenu ainsi: on prend $X = Y =$ courbe elliptique, $p(x) = 2x$ (au sens de la loi du groupe), de sorte que X devient un révêtement à 4 feuillets de Y, et on prend pour E un fibré extension non triviale du fibré en droites défini par le diviseur (P) (P un point de Y) par le fibré en droites trivial. (Le fait que $p^{-1}(E)$ est décomposable peut être prouvé à l'aide des résultats de Atiyah, Proc. London Math. Soc. 1955).

BOUNDED MATRICES AND LINEAR DIFFERENTIAL EQUATIONS.*

By Aurel Wintner.

The following considerations deal with ordinary (homogeneous) linear differential equations in Hilbert space, with coefficient matrices which are bounded. It is well-known that the choice of bounded "matrices," instead of bounded "operators," is not a loss of generality. Some of the results to be obtained seem to be new in the case of finite matrices also.

1. Let $x_1, x_2, \cdots$ be complex numbers, $x = (x_1, x_2, \cdots)$ a vector in Hilbert's space ($|x| < \infty$), every capital $C, F, \cdots$ a bounded matrix, $|C|$ the least upper bound of the length $|Cx|$ of the vector Cx when $|x| = 1$ (so that $|C| < \infty$), and C° the (bounded, Hermitian) matrix $\frac{1}{2}(C + C^*)$. If $C(x, y)$ denotes the bilinear form determined by C, then the real part of the value of the form $C(x, \bar{x})$ is identical with that of the Hermitian form $C^{\circ}(x, \bar{x})$, since, if C_o is defined by $C = C^{\circ} + C_o$, then $C_o^* = -C_o$, hence $\operatorname{Re} C_o(x, \bar{x}) = 0$. Clearly, $C = C^{\circ}$ if and only if C is Hermitian. It also follows from

$$\operatorname{Re} C(x, \bar{x}) = C^{\circ}(x, \bar{x}) \tag{1}$$

that if λ denotes the least, and μ the greatest, value occurring in the spectrum of the Hermitian matrix C°, then, since λ is known to be the greatest lower, and μ the least upper, bound of $C^{\circ}(x, \bar{x})$ for $|x| = 1$,

$$\lambda |x|^2 \leqq \operatorname{Re} C(x, \bar{x}) \leqq \mu |x|^2. \tag{2}$$

The (finite, non-negative) difference $\mu - \lambda$, *the real spectral span of* C, will be denoted by $[C]$; so that

$$[C] = \underset{|x|=1}{\text{l.u.b.}} \operatorname{Re} C(x, \bar{x}) - \underset{|x|=1}{\text{g.l.b.}} \operatorname{Re} C(x, \bar{x}), \tag{3}$$

hence

$$[C] = [C^{\circ}], \text{ where } C^{\circ} = \tfrac{1}{2}(C + C^*). \tag{3 bis}$$

C is called non-singular if there exists a *unique* bounded C^{-1} satisfying $CC^{-1} = I$ and/or $C^{-1}C = I$, where I is the unit matrix.

* Received October 31, 1956.

2. If there is given a bounded matrix $C = C(t)$ at every point t of an interval $0 \leqq t < \omega$, where $\omega \leqq \infty$, and if $|C(t_n) - C(t)| \to 0$ as $n \to \infty$ holds for every fixed t whenever $t_n \to t$, then $C(t)$ will be called continuous. Starting with such a $C(t)$ and denoting dx/dt by x', consider for the vector $x = x(t)$ the differential equation

$$x' = C(t)x \tag{4}$$

with an initial condition $x(0)$ satisfying $|x(0)| < \infty$. It is well-known (cf. [5], p. 1477, or [3], pp. 681-684, where further references are given) that this initial value problem has a unique solution $x = x(t)$, satisfying $|x(t)| < \infty$, on the entire interval $0 \leqq t < \omega$. The proof of these assertions is word by word the same as in the case of the finite-dimensional case, since both the customary existence proofs, such as that based on successive approximations, and the uniqueness argument of Lipschitz are applicable without any change.

What is somewhat less straightforward is the transfer to the case of Hilbert's space of the main theorem on the "fundamental matrices" $X(t)$ of (1), since, in the finite-dimensional case, the proof of that theorem is usually based on the identity

$$d(t) = d(0) \exp \int_0^t \operatorname{tr} C(s)\, ds, \text{ where } d(t) = \det X(t), \tag{5}$$

(Jacobi-Liouville), an identity which is not available in the general case. For a simple argument replacing the use of (5), cf. Section 4 below.

3. A vector $x(t)$ will not be considered a solution of (4) unless $|x(t)| < \infty$ for $0 \leqq t < \omega$. This implies that $|x(t)| > 0$ throughout unless $x(t)$ is the trivial solution, $x(t) \equiv 0$. In fact, if $0 \leqq t_0 < \omega$, then $x(t) \equiv 0$ is a solution of (4) satisfying the initial condition $x(t_0) = 0$, and so the assertion follows from the uniqueness theorem. Let $x(t)$ be any solution of (4) distinct from the trivial solution; so that

$$0 < r(t) < \infty \text{ for } 0 \leqq t < \omega, \text{ where } r = \tfrac{1}{2}|x|^2. \tag{6}$$

Under the assumption that $C = C(t)$ is continuous for $0 \leqq t < \omega$, let $\lambda = \lambda(t)$ and $\mu = \mu(t)$, where t is fixed, be the least and greatest values occurring in the spectrum of the Hermitian matrix $C^0 = C^0(t)$, where $C^0 = \frac{1}{2}(C + C^*)$. Then multiplication of (4) and of the complex conjugate

of (4) by $\bar{x} = \bar{x}(t)$ and $x = x(t)$ respectively, when followed by an application of (1) and (2), shows that

$$2\lambda(t)r(t) \leqq r'(t) \leqq 2\mu(t)r(t) \quad \text{for } 0 \leqq t < \omega, \tag{7}$$

by (6). Since $r'(t)/r(t)$ is the derivative of $\log r(t)$, it is clear from (6) and (7) that

$$| x(0) | \exp \int_0^t \lambda(s)\,ds \leqq | x(t) | \leqq | x(0) | \exp \int_0^t \mu(s)\,ds, \tag{8}$$

where $0 \leqq t < \omega$, holds for the length of every solution $x(t)$ of (4).

In [16], pp. 558-559, this inequality was derived, for a certain asymptotic purpose, in the finite-dimensional case (for later references, cf. [2], pp. 20-22, or [17], Section 2). But the proof has nothing to do with this restriction and, although both the proof and the assertion of (8) are simple indeed, the central position of (8) in the theory of (4) has not been noted in the literature. It will be seen that the consequences of (8) are manifold.

The simplest consequence of (8) results if (8) is applied to the case $C(t) =$ const. of (4). Then (8) reduces to an inequaliy deduced by Heinz [4], pp. 426-427, by arguments which are applicable in the particular case $C(t) =$ const.; cf. Section 5 below.

4. Let $X(t)$ denote a matrix of the form $(x^1(t), \cdots, x^m(t), \cdots)$ in which every column vector $x^m(t)$ is a solution $x(t)$ of (4). If the initial data $x^1(0), \cdots, x^m(0), \cdots$ are so chosen that $X(0)$ is a bounded matrix, then $X(t)$ will be called a solution matrix of (4). If, in addition, $X(0)$ is chosen to be non-singular (cf. the end of Section 1), then $X(t)$ will be called a fundamental matrix of (4). It will be concluded from (8) that if t is fixed on the interval $0 < t < \omega$, then the matrix $X(t)$ is (a) a bounded matrix for every solution matrix and (b) a non-singular matrix in case of a fundamental matrix. Assertion (b) is the fact which, in the finite-dimensional case, is usually concluded from (5).

With reference to a fixed m, let $X_m(t)$ denote the solution matrix corresponding to which the k-th column of $X_m(0)$ is the vector 0 or the k-th column of the unit matrix I according as $m < k < \infty$ or $1 \leqq k \leqq m$. Then, if the definition of $| C |$ (cf. the first sentence of Section 1) is applied to $C = X_m(t)$, it is readily seen from (8) that, in view of the superposition principle of (4), both inequalities

$$(9) \qquad \exp \int_0^t \lambda(s)\,ds \leqq |X(t)| \leqq \exp \int_0^t \mu(s)\,ds, \text{ where } 0 \leqq t < \omega,$$

hold for $X(t) = X_m(t)$. Hence, if $m \to \infty$, and if $X(t)$ now denotes the fundamental matrix determined by the initial condition

$$(10) \qquad X(0) = I,$$

then (9) holds for this $X(t)$ also. In particular, the second of the inequalities (9) shows that this $X(t)$ is a bounded matrix for every non-negative $t < \omega$. But it also follows from (10) that the solution $x(t)$ of (4) belonging to an arbitrary initial vector $x(0)$ (with $|x(0)| < \infty$) is

$$(10\text{ bis}) \qquad x(t) = X(t)x(0), \text{ where } 0 \leqq t < \omega,$$

and that, correspondingly, the most general solution matrix [fundamental matrix] of (4) is $X(t)A$, where $A =$ const. is an arbitrary [non-singular] bounded matrix.

This, when combined with the relations $|B_1B_2| \leqq |B_1||B_2|$ and $|I| = 1$ (and with the choice $B_1 = B$, $B_2 = B^{-1}$ when B is non-singular), proves both of the assertions (a)-(b). In fact, (a) follows in a refined form, according to which

$$(11) \qquad |X(t)| \leqq |X(0)| \exp \int_0^t \mu(s)\,ds, \text{ where } 0 \leqq t < \omega,$$

holds for every solution matrix $X(t)$, and (b) follows in a refined form, acocrding to which

$$(12) \qquad |X^{-1}(t)| \leqq |X^{-1}(0)| \exp \int_0^t -\lambda(s)\,ds, \text{ where } 0 \leqq t < \omega,$$

holds for every fundamental matrix.

5. The simplest corollary of (11) is the inequality of Heinz, referred to at the end of Section 3. It states that, if A is any bounded matrix,

$$(13) \qquad |e^A| \leqq \exp \operatorname*{l.\,u.\,b.}_{|x|=1} A^0(x, \bar{x}), \text{ where } A^0 = \tfrac{1}{2}(A + A^*)$$

(e^A is defined by $I + \cdots + A^n/n! + \cdots$). In fact, if the numbers λ, μ denote the best bounds satisfying the case $C = A$ of (2) (for every x), then (13) is equivalent to the first of the two inequalities

$$(14) \qquad |e^A| \leqq e^{\mu}, \qquad |e^{-A}| \leqq e^{-\lambda}.$$

If the coefficient matrix $C(t)$ of (4) is chosen to be the given bounded $A = \text{const.}$ (the t-interval can be chosen to be the half-line $0 \leqq t < \infty$), then the fundamental matrix $X(t)$ belonging to (10) is $X(t) = e^{tA}$. Hence, if λ, μ are the constants defined before (14), then (11) and (12) reduce to $|e^{tA}| \leqq e^{\mu t}$ and $|(e^{tA})^{-1}| \leqq e^{-\lambda t}$, and so (14) follows by choosing $t = 1$.

6. It is possible to reduce the second of the inequalities (14) to the first, which is (13) (cf. Heinz, [4], pp. 426-428, and the end of Section 8 below). In any case, both parts of (14) are involved in the following estimate, which will be needed below: If T is a non-singular matrix of the form e^A, where A is bounded matrix, and if F is any bounded matrix, then

(15) $$|TFT^{-1}| \leqq e^{[A]}|F|, \text{ where } T = e^A$$

Here $[A]$ denotes the "real spectral span" of A, as defined in Section 1. Hence $e^{[A]} = e^{\mu-\lambda}$ in the notations used in (14). Thus it is clear from $|B_1B_2B_3| \leqq |B_1||B_2||B_3|$ that (15) follows from (14).

7. As proved in [14] (in this connection, cf. [13], pp. 281-282, and the end of p. 267), there belongs to every bounded, non-singular T a unique unitary $U = (U^*)^{-1}$ and a unique (bounded) positive definite $P = P^*$ satisfying $T = PU$. It turns out that, in terms of the $P = P_T$ of T, it is possible to formulate the estimate (5) of the *affine distortion* of a bounded matrix F in such a way as to dispose of the hypothesis implicit in (15), viz., of the restriction that T, besides being non-singular, be such as to possess a bounded logarithm ($= A$) or, what is the same thing, that T be embeddable (as T^1) into a continuous cyclic semi-group of bounded matrices T^t, where $0 \leqq t < \infty$.

The resulting generalization of (15) is as follows: If T and F are bounded, and if T is non-singular, then

(16) $$|TFT^{-1}| \leqq [P]|F|,$$

where $[P]$ is the (real) spectral span of the positive definite factor $P = P^*$ in $T = PU$.

First, as pointed out in [13], p. 267, there belongs to every bounded, positive definite $P = P^*$ a unique bounded $Q = Q^*$ satisfying $P = e^Q$, and the spectrum of this Q consists of the (real) logarithms of the values occurring in the spectrum of P. In particular, $[P] = e^{[Q]}$. Hence the assertion (16), where $T = PU$, is equivalent to

(16 bis) $$|e^QUFU^{-1}e^{-Q}| \leqq e^{[Q]}|F|.$$

But the truth of (16 bis) follows from the case $T = e^Q$ of (15), since, U being unitary, $|UFU^{-1}| = |F|$.

8. If H is bounded and Hermitian, then the same is true of e^H, and e^H is positive definite, since, in view of the spectral resolution of H, a value a is in the spectrum of H if and only if e^a is in the spectrum of e^H (and since, every a being real, every e^a is positive). Similarly, e^{iH} is a unitary matrix and, as first proved in [13], pp. 268-277, every unitary matrix can be represented in the form e^{iH}.

If A is bounded, then there exists a unique pair of bounded Hermitian matrices H, K satisfying $A = H + iK$; in fact, $H = A^0$, $K = A_0$ in the notations of Section 1. Let e^H and e^{iK} be denoted by P and U respectively. Then $PU = UP = e^A$ if $HK = KH$ (that is, if A is normal). In this case and, more generally, if $e^{H+iK} = PU$ happens to be true, it is clear from $|B_1B_2| \leqq |B_1||B_2|$ and $|U| = 1$ that $|e^A| \leqq |P|$.

It turns out, however, that the last inequality is true for *every* bounded A; in other words, *if A is bounded, and if $H = H^*$ and $K = K^*$ are defined by $A = H + iK$, then $|e^{H+iK}| \leqq e^H$.* In fact, since e^H is positive definite (cf. the beginning of this Section 8), there exists a unique (bounded) positive definite Q satisfying $e^H = e^Q$ (cf. Section 7), and so the last italicized statement is equivalent to the first of the relations (14), where $A = K + iH$. The second of the relations (14) follows if A is replaced by $-A$ in the last italicized assertion.

9. In what follows, the asymptotic behavior (as $t \to \infty$) of the solution vectors (xt) of (4) will be considered, when appropriate restrictions are placed on the behavior of the coefficient matrix $C(t)$. *It will always be assumed that $0 \leqq t < \infty$, and that the matrix $C(t)$ is bounded and continuous for fixed t* (but neither $|C(t)| <$ const. as $t \to \infty$ nor the uniform continuity of $C(t)$ for $0 \leqq t < \infty$ will be assumed).

(i) *In terms of a given $C = C(t)$, where $0 \leqq t < \infty$, define $C^0 = C^0(t)$ by $C^0 = \frac{1}{2}(C + C^*)$ (so that $(C^0)^* = C^0$), and $\lambda = \lambda(t)$, $\mu = \mu(t)$ by placing*

$$(17) \qquad \lambda = \underset{|x|=1}{\text{g. l. b.}}\, C^0(x, \bar{x}), \qquad \mu = \underset{|x|=1}{\text{l. u. b.}}\, C^0(x, \bar{x})$$

(for fixed t). Suppose that both integrals

$$(18) \qquad \int_0^\infty \lambda(t)\,dt, \quad \int_0^\infty \mu(t)\,dt, \quad \text{where} \quad \int_0^\infty = \lim_{t\to\infty} \int_0^t,$$

are convergent (both $\int^{\infty} |\lambda(t)|\, dt = \infty$ *and* $\int^{\infty} |\mu(t)|\, dt = \infty$ *are allowed). Then the length* $|x(t)|$ *of every solution vector* $x(t) \not\equiv 0$ *of* (4) *tends to a finite and non-vanishing limit as* $t \to \infty$.

This follows by replacing $s = 0$ and $s = t$ in (8) by $s = u$ and $s = v$ respectively, and then letting $v - u \to \infty$.

(ii) *If* $C(t)$ *satisfies the assumptions of* (i), *then there belongs to every fundamental matrix* $X(t)$ *of* (4) *a pair of constants satisfying* $|X(t)| < \text{const.}$ *and* $|X^{-1}(t)| < \text{Const.}$ *as* $t \to \infty$.

This is clear from (11) and (12).

(iii) *The assumptions imposed on* $C(t)$ *in* (i) *and* (ii) *are satisfied if (but not only if)*

(19) $$\int_0^{\infty} |C^0(t)|\, dt < \infty, \text{ where } C^0 = \tfrac{1}{2}(C + C^*).$$

In fact, (19) is sufficient for the *absolute* convergence of the integrals (18), since it follows from (17) that $|\lambda| \leqq |C^0|$, $|\mu| \leqq |C^0|$.

10. The assumption (19) puts no restriction on the "skew-symmetric" component of C; that is, on the matrix which, in Section 1, was denoted by C_0. Correspondingly,

(20) $$\int_0^{\infty} |C(t)|\, dt < \infty$$

is an assumption which is even stricter than (19). It turns out that, if (20) is assumed, then much more than what is assured by (i) and (ii) can be asserted:

(iv) *If the coefficient matrix* $C(t)$ *of* (4) *satisfies* (20), *then*

(21) $$X(t) \to I \text{ as } t \to \infty$$

holds for a certain (unique) fundamental matrix $X(t)$ *of* (4).

In the case of finite matrices, the assertion of (iv) is well-known; it goes back to Bôcher and Dunkel (cf. their papers, referred to in the first two footnotes in [7], p. 486, to which I called attention some time ago). The following proof is so primitive as to hold for bounded matrices also.

Let $X(t)$ be any fundamental matrix of (4). Then, since (20) is sufficient for (19), it follows from (iii) that (ii) is applicable. But since (4) is equivalent to $X'(t)=C(t)X(t)$, it follows from (20) and from the first of the assertions of (ii) that, since $|CX|\leqq|C||X|$,

$$\int_0^\infty |X'(t)|\,dt<\infty;\ \text{in particular,}\ \int_0^\infty X'(t)dt=\lim_{s\to\infty}\int_0^s dX(t)$$

is convergent; that is, $X(\infty)=\lim X(s)$, where $s\to\infty$, exists in the weak sense, to begin with. But the first assertion of (ii) assures that $X(\infty)$ is a bounded matrix, and the second assertion of (ii) shows that $X(\infty)$ is non-singular. Hence, it is sufficient to replace the given fundamental matrix $X(t)$ by $X(t)X^{-1}(\infty)$ in order to obtain the fundamental matrix satisfying (21).

11. By Lagrange's device of the variation of constants (in this regard, cf. [15], pp. 190-191), the following criterion on "small perturbations" can now be concluded:

(v) *For every fixed t, where $0\leqq t<\infty$, let $C(t)$ and $B(t)$ be bounded and continuous. Suppose that, for large t, the matrix $C(t)-B(t)$ is so "small" with reference to a fundamental matrix $X(t)$ of $x'=C(t)x$ that*

$$\int_0^\infty |G(t)|\,dt<\infty,\ \text{where}\ G=X^{-1}(C-B)X. \tag{22}$$

Then $y'=B(t)y$ possesses a fundamental matrix $Y(t)$ of the form

$$Y(t)=X(t)(I+Z(t)),\ \text{where}\ \lim_{t\to\infty}|Z(t)|=0. \tag{23}$$

Due to (iv), the proof of (v) is the same as the proof given in [15], pp. 200-201 (where the matrices are finite), and can therefore be omitted.

12. If (v) is combined with (15), then there results an asymptotic statement which seems to be new even in case of finite matrices. In fact, a result of [15], pp. 188-196 (1946) and the similar, but less inclusive, results of Erugin (1946; cf. [11], pp. 176-182), apply, in case of finite matrices, in the same direction as (vi) below but are weaker than what (vi) becomes in the case of finite matrices.

(vi) *Let $[A]$ denote the real spectral span of a bounded matrix* $A=\text{const.}$ *and let $F(t)$, where $0\leqq t<\infty$, be a matrix which, for every fixed t, is bounded and continuous. Suppose that*

$$(24)\qquad \int_0^\infty e^{[A]t}\,|\,F(t)\,|\,dt < \infty$$

(where $|\,F\,| = \text{l.u.b.}\,|\,Fx\,|$ *for* $|\,x\,| = 1$*). Then the case* $C(t) = A + F(t)$ *of* (4) *possesses a fundamental matrix* $X(t)$ *of the form*

$$(25)\qquad X(t) = e^{tA}(I + Z(t)),\ \text{where}\ \lim_{t\to\infty} |\,Z(t)\,| = 0.$$

In order to prove this, let the A and $F(t)$ in (vi) be identified with the $C(t)$ and $B(t)$ of (v) respectively. The $Y(t)$ of (v) becomes the $X(t)$ of (vi), and the $X(t)$ of (v) can be chosen to be e^{tA}, since e^{tA} is a fundamental matrix of the case $C(t) = A$ of (4). Accordingly, (23) and (22) go over into (25) and

$$(26)\qquad \int_0^\infty |\,e^{-tA}F(t)e^{tA}\,|\,dt < \infty$$

respectively. Consequently, (vi) follows from (v) if it is ascertained (24) is sufficient for (26). But it is clear from (3) that $|\,tA\,| = |\,t\,|\,A$. Hence, the sufficiency of (24) for (26) follows if A is replaced by $-tA$ in (15).

13. Let $\lambda = \text{const.}$ be the greatest lower bound of (1) for $|\,x\,| = 1$, where $C = \text{Const.}$ is any bounded matrix. Then Satz 6 of Heinz ([4], p. 428; cf. [10], passim) states that if $\lambda > 0$, then C is non-singular and, in addition,

$$(27)\qquad C^{-1} = \int_0^\infty e^{-tC}\,dt$$

and $|\,C^{-1}\,| \leqq \lambda^{-1}$. Heinz points out that the first of these assertions, that preceding (27), is a refinement of a result of Toeplitz, and he mentions certain recent references concerning this refinement. But neither [4] nor [10] mentions that this (viz., the existence of a unique, bounded C^{-1} if $\lambda > 0$) is contained, in a substantially improved form, in the results of [13], and that, corresponding to this improvement, (27) can be improved to the following assertion: *If A is bounded, then the Liouville-Neumann expansion*

$$(28)\qquad (zI - A)^{-1} = \sum_{n=0}^{\infty} z^{-n-1}A^n$$

(which is certainly valid, in the sense of convergence, outside the circle $|\,z\,| \leqq |\,A\,|$) *is valid, in the sense of* (*absolute*) *Borel summability, outside the least convex region containing those complex numbers z for which $zI - A$ is non-singular*; cf. Section 15 below.

What is today generally called the spectrum of an arbitrary bounded C was first defined in [13], p. 239, as the set $\sigma(C)$ of those complex numbers z for which $zI - C$ fails to be non-singular. It was proved in [13], pp. 242-243, that $\sigma(C)$ is a closed bounded set which contains at least one point. There is a curious oversight in [12], p. 149 (repeated in [10], pp. 409-412 and disguised in [8]): both the definition of $\sigma(C)$ and the proof for the existence of $\sigma(C)$ are *verbatim* the same in [13].

Let $\rho(C)$ denote the closure of the set of the (complex) values attained by the bounded form $C(x, \bar{x})$ when $|x| = 1$. For finite matrices C, it was conjectured by Toeplitz, and proved by Hausdorff, that

$$\rho(C) \text{ is convex,} \tag{29}$$

and it was proved by Toeplitz that

$$\sigma(C) \text{ is a subset of } \rho(C). \tag{30}$$

When Toeplitz proved (30) for finite matrices, the definition of $\sigma(C)$ for bounded matrices was not in the literature, and if it would have been, his proof, having been based on eigenvectors, could not have led to (30) for bounded C. But it was shown in [13], p. 245, that the definition of $\sigma(C)$, introduced in [13], p. 239, is such as to lead to the truth of (30) for any bounded C. In contrast, the truth of (30) for every bounded C was clear from the beginning, since it is implied by the truth of (30) for every finite C; cf. [13], p. 244.

14. If H is a bounded Hermitian matrix, then $\sigma(H)$ is a bounded set of real numbers which, in view of (29), is an interval and about which the spectral resolution of H impiles that $\rho(H)$ is the *least* interval containing $\sigma(H)$ (cf. [13], p. 250; this cannot be concluded from (30) alone).

If this is applied to $H = C^{\circ}$, then it is clear from (29), (30) and (1) that $z = 0$ cannot be in $\sigma(C)$ if it is not in $\rho(C^{\circ})$. This means that C must be non-singular if C° is positive definite (or negative definite), that is, if $\lambda > 0$ (or $\mu < 0$) in (17). This is the result quoted before (28).

15. Let $\tau(C)$ denote the convex closure of $\sigma(C)$. Then it is clear from (30) and (29) that

$$\tau(C) \text{ is a subset of } \rho(C). \tag{31}$$

The fact referred to at the beginning of Section 14 is equivalent to the statement that (31) can be replaced by

(32) $$\tau(H) = \rho(H) \text{ if } H = H^*$$

(the same holds for normal matrices; cf. [13], p. 282.)

The result of Heinz, quoted in connection with (27), states that if λ is the least value occurring in the set (32) when $H = C^{\circ}$, then $\lambda > 0$ implies that C is non-singular, that (27) holds, and that $|C^{-1}| \leqq 1/\lambda$. Hence, if C is replaced by $zI - C$, and if λ_z denotes the least value occurring in the set (32) when $H = (zI - C)^{\circ}$, then $\lambda_z > 0$ implies that $z = 0$ is not in $\tau(C)$, that

(33) $$(zI - C)^{-1} = \int_0^{\infty} e^{-t(zI-C)}\, dt,$$

and that

(34) $$|(zI - C)^{-1}| \leqq 1/\lambda_z.$$

Thus, if C is replaced by $e^{i\phi}C$, where ϕ is an arbitrary real scalar, then, by comparing the supporting function of the convex set $\tau(C)$ with the supporting function of Borel's convex "indicatrix" (of a power series of non-vanishing radius of convergence; cf. [1], pp. 120-129; [9], pp. 578-593), it is readily found that (28) is valid, in the sense of Borel's (absolute) summation process, precisely on the z-domain which is the complement of the (closed, bounded) set $\tau(C)$. In fact, $(zI - C)^{-1}$ is a "(bounded) regular function" on the complement of $\sigma(C)$. For, on the one hand, $\tau(C)$ contains $\sigma(C)$ and, on the other hand, $(zI - C)^{-1}$ can be expanded, in a sufficiently small circle $|z - z_0| < \gamma = \gamma(z_0)$, into a "(bounded) regular power series" in $z - z_0$, if z_0 is any point in the complement of $\tau(C)$; cf. [13], p. 242 and pp. 245-247.

It should be emphasized that, in view of (31), the Borel summability in $z - z_0$, if z_0 is any point in the complement of $\sigma(C)$; cf. [13], p. 242 and be concluded from, the Borel summability of (28) on the complement of $\rho(C)$.

Appendix.

Let a bounded A be called logarithmizable, or an l-matrix, if there exists some bounded C for which $A = e^C$ holds. Every l-matrix is non-singular (in fact, $Be^C = I$ and $e^C B = I$ are satisfied by the bounded matrix $B = e^{-C}$). Around 1929 I raised the question whether the converse is also

true (as it is in case of finite matrices, in which case the customary proofs depend on the theory of elementary divisors or, at least, on the theorem of Hamilton-Cayley; cf. however [19], p. 364). Now it is finally sure that the answer is in the negative:

In order that a bounded matrix be logarithmizable, it is (necessary but) not sufficient that it be non-singular.

In fact, it is clear (cf. the end of p. 361 in [19]) that an A cannot be an l-matrix unless there exists some bounded B satisfying $A = B^2$. But it was recently shown by Halmos, Lumer and Schäffer [18] that for certain (bounded) non-singular A there will not exist such a B.

Accordingly, the l-matrices form a *proper* subset of the group of all non-singular matrices. Is this subset a group? The answer to this question, too, proves to be negative:

The logarithmizable matrices fail to form a group.

In fact, it was proved in [13], pp. 268-277 and p. 267, that every unitary U and every positive definite (non-singular) $P = P^*$ is an l-matrix. On the other hand, as shown in [14], every non-singular A has a unique factorization of the form $A = PU$. Hence, if the product of two l-matrices were always an l-matrix, it would follow that every non-singular A is an l-matrix.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] E. Borel, *Leçons sur les séries divergentes*, Paris, 1901.

[2] R. Conti, "Sulla stabilità dei sistemi di equazioni differenziali lineari," *Rivista di Matematica della Università di Parma*, vol. 6 (1955), pp. 3-34.

[3] H. Hamburger, "Zur Theorie der sphärischen Abbildung im Grossen. I," *Mathematische Zeitschrift*, vol. 31 (1930), pp. 629-708.

[4] E. Heinz, "Beiträge zur Störungstheorie der Spektralzerlegung," *Mathematische Annalen*, vol. 123 (1951), pp. 415-438.

[5] E. Hellinger and O. Toeplitz, "Grundlagen für eine Theorie der unendlichen Matrizen," *Mathematische Annalen*, vol. 69 (1910), pp. 289-330.

[6] ———, Article II C1. 13 (1927) in the Encyclopädie der mathematischen Wissenschaften, vol. II, part 3_2.

[7] E. Hilb, Article II B 5 (1913) in the Encyclopädie der mathematischen Wissenschaften, vol. II, part 2.

[8] J. von Neumann, "Eine Spektraltheorie für allgemeine Operatoren eines unitären Raumes," *Mathematische Nachrichten*, vol. 4 (1951), pp. 258-281.

[9] G. Pólya, "Untersuchungen über Lücken und Singularitäten von Potenzreihen," *Mathematische Zeitschrift*, vol. 29 (1929), pp. 549-640.

[10] F. Riesz and B. Sz.-Nagy, *Leçons d'analyse fonctionnelle*, third edition, Paris, Budapest, 1955.

[11] V. V. Stepanoff and V. V. Nemitsky, *Qualitative theory of differential equations* (in Russian), Moscow, 1949.

[12] M. H. Stone, *Linear Transformations in Hilbert Space*, New York, 1932.

[13] A. Wintner, "Zur Theorie der beschränkten Bilinearformen," *Mathematische Zeitschrift*, vol. 30 (1929), pp. 228-289.

[14] ———, "On non-singular bounded matrices," *American Journal of Mathematics*, vol. 54 (1932), pp. 142-149.

[15] ———, "Linear variations of constants," *ibid.*, vol. 68 (1946), pp. 185-213.

[16] ———, "Asymptotic integration constants," *ibid.*, vol. 68 (1946), pp. 553-559.

[17] ———, "Energy dissipation and linear stability," *Quarterly of Applied Mathematics*, to appear.

APPENDIX.

[18] P. Halmos, G. Lumer, and J. J. Schäffer, "Square roots of operators," *Proceedings of the American Mathematical Society*, vol. 4 (1953), pp. 142-149; cf. P. Halmos and G. Lumer, Part II, *ibid.*, vol. 5 (1954), pp. 589-595.

[19] A. Wintner, "On the logarithms of bounded matrices," *American Journal of Mathematics*, vol. 74 (1952), pp. 360-364.

A NOTE ON ENTROPY.*

By I. I. Hirschman, Jr.[1]

Let $\| f \| = \left(\int_{-\infty}^{\infty} | f(x) |^2 \, dx \right)^{\frac{1}{2}}$, where $f(x) \in L^2(-\infty, \infty)$ and let

$$f(x) \sim \int_{-\infty}^{\infty} g(y) e^{2\pi i x y} \, dy, \qquad g(y) \sim \int_{-\infty}^{\infty} f(x) e^{-2\pi i x y} \, dx, \tag{1}$$

where the $\sim$ refers to convergence in the mean of L^2 (*Plancherel*); so that $\| f \| = \| g \|$. If

$$\| f \| = \| g \| = 1, \tag{2}$$

then $| f(x) |^2$ and $| g(y) |^2$ may be considered as probability frequency functions. The variance $V[\phi]$ of a frequency function is defined by

$$V[\phi] = \int_{-\infty}^{\infty} (x - m)^2 \phi(x) \, dx, \text{ where } m = \int_{-\infty}^{\infty} x \phi(x) \, dx$$

is the mean value. $V[\phi]$ may be taken as a measure of the "concentration" of ϕ in the neighborhood of its mean, a small value of V corresponding to a high degree of concentration. Weyl, [4], has shown that not both of the frequency functions $| f(x) |^2$ and $| g(y) |^2$ can be highly concentrated in this sense and that in fact

$$V[| f(x) |^2] V[| g(y) |^2] \geqq 1/16\pi^2,$$

a relation having application to the uncertainty principle of quantum mechanics.

In this note we shall demonstrate a similar result concerning entropy. The entropy $E[\phi]$ of a frequency function $\phi(x)$ is

$$E[\phi] = \int_{-\infty}^{\infty} \phi(x) \log \phi(x) \, dx.$$

Entropy is a measure of concentration of ϕ on a set of small measure, a large positive value of E corresponding to a high degree of concentration.

---

* Received August 16, 1956.

[1] This research was supported in part by the Office of Scientific Research and Development Command of the United States Air Force under contract.

We shall show that in the sense of entropy $|f(x)|^2$ and $|g(y)|^2$ cannot both be highly concentrated. More precisely we shall prove the following result.

THEOREM. *Under the assumptions* (1) *and* (2),

$$E[|f(x)|^2]+E[|g(y)|^2]\leqq 0 \tag{3}$$

whenever the left hand side has meaning.

There are heuristic arguments which suggest that the extremal functions in the inequality (3) are $f(x)=\pi^{-\frac{1}{4}}e^{-x^2/2}$ and its dilations. Consequently our theorem may hold with the improved conclusion

$$E[|f(x)|^2]+E[|g(y)|^2]\leqq \log 2-1. \tag{4}$$

However I have not been able to establish this. If this inequality is valid in this form then it includes the inequality of Weyl since for any frequency function $\phi(x)$ we have

$$E[\phi]\geqq -\tfrac{1}{2}-\tfrac{1}{2}\log\{2\pi V[\phi]\}. \tag{5}$$

See [2]. More generally if

$$M_{a,p}[\phi]=[\int_{-\infty}^{\infty}|x-a|^p\phi(x)\,dx]^{1/p} \qquad (-\infty<a<\infty, 0<p<\infty),$$

then the argument used to prove (5) shows that

$$E[\phi]\geqq -\log A(p)-\log M_{a,p}[\phi], \text{ where } A(p)=2p^{(1-p)/p}e^{1/p}\Gamma(1/p).$$

Using (3) we find that for $0<p<\infty$, $0<q<\infty$,

$$M_{a,p}[|f(x)|^2]M_{b,q}[|g(y)|^2]\geqq 1/A(p)A(q).$$

However the inequalities obtained, even if (4) is used in place of (3), are clearly not best possible except when $p=q=2$.

For further studies of the "concentration" of pairs of Fourier transforms, see the paper of W. H. Fuchs [1].

We now turn to the demonstration of Theorem 1. Let us agree that $E[|f(x)|^2]$ is defined whenever one of the integrals

$$\int_{-\infty}^{\infty}|f(x)|^2\log^+|f(x)|^2\,dx, \qquad \int_{-\infty}^{\infty}|f(x)|^2\log^-|f(x)|^2\,dx$$

is finite. The left hand side of (3) therefore has meaning except in the following two cases: a. one of $E[|f(x)|^2]$ or $E[|g(y)|^2]$ is undefined; b. one of $E[|f(x)|^2]$ and $E[|g(y)|^2]$ is $+\infty$ and the other $-\infty$.

Our demonstration consists in subjecting the integral form of the Young-Hausdorff inequality, see [5], to that limit process which leads from the powers of a positive number to its logarithm. We begin by supposing that $f(x) \in L^1(-\infty, \infty) \cap L^2(-\infty, \infty)$. Let $p^{-1} + q^{-1} = 1$. We set

$$C(p) = q^{-1} \log[\int_{-\infty}^{\infty} | g(y)|^q dy] - p^{-1} \log[\int_{-\infty}^{\infty} | f(x)|^p dx].$$

By the Young-Hausdorff theorem (the extension to Fourier transforms is due to Titchmarsh), $C(p) \leqq 0$, if $1 < p \leqq 2$. Parseval's equality gives $C(2) = 0$, and these together show that $C'(2-) \geqq 0$, if, of course, $C'(2-)$ exists.

For each x the function

$$[| f(x)|^2 - | f(x)|^p]/(2-p) \tag{6}$$

increases to $| f(x)|^2 \log | f(x)|$ as $p \uparrow 2-$. Since the function (6) is integrable for any fixed $p < 2$ it follows that

$$\text{if } A(p) = \int_{-\infty}^{\infty} | f(x)|^p dx, \text{ then } A'(2-) = \int_{-\infty}^{\infty} | f(x)|^2 \log | f(x)| \, dx,$$

where $A'(2-)$ is always defined, $-\infty < A'(2-) \leqq +\infty$. Similarly,

$$\text{if } B(q) = \int_{-\infty}^{\infty} | g(y)|^q dy, \text{ then } B'(2+) = \int_{-\infty}^{\infty} | g(y)|^2 \log | g(y)| \, dy,$$

where $B'(2+)$ is always defined, $-\infty \leqq B'(2) < +\infty$.

From $C(p) = q^{-1} \log B(q) - p^{-1} \log A(p)$, $(p^{-1} + q^{-1} = 1)$,

$$C'(2-) = -\tfrac{1}{2} B'(2+) - \tfrac{1}{2} A'(2-). \tag{7}$$

Here we have used $B(2) = A(2) = 1$. The relation (7) in conjunction with the inequality $C'(2-) \geqq 0$ shows that (3) holds except in the case when $E[f] = +\infty$ and $E[g] = -\infty$.

If it is no longer assumed that the quantities

$$\| f \|^2 = \int_{-\infty}^{\infty} | f(x)|^2 dx = \int_{-\infty}^{\infty} | g(y)|^2 = \| g(y)\|^2$$

are 1 then our relation becomes

$$E[| f |^2] \| f \|^{-2} + E[| g |^2] \| g \|^{-2} \leqq \log \| f \|^2 + \log \| g \|^2. \tag{8}$$

We now abandon our assumption that $f(x) \in L^1(-\infty, \infty)$. It is sufficient to consider the case when $E[| f |^2]$ and $E[| g |^2]$ are defined. Let $\omega_T(x)$ be $1 - | x | T^{-1}$ for $| x | \leqq T$ and 0 for $| x | > T$, and let $\Omega_T(y)$

$=\sin^2 \pi Ty/(\pi^2 Ty^2)$ be the Fourier transform of $\omega_T(x)$. The functions $\omega_T(x)f(x)$ and $\Omega_T(y)*g(y)$ are Fourier transforms of each other and $\| \omega_T(x)f(x) \| = \| \Omega_T(y)*g(y) \| \leqq 1$. Since $\omega_T(x)f(x) \in L^1(-\infty, \infty)$ we may apply (10) to conclude that either

$$E[|\omega_T(x)f(x)|^2] + E[\Omega_T(y)*g(y)|^2] \leqq 0 \tag{9}$$

holds or $E[|\omega_T f|^2] = +\infty$ and $E[|\Omega_T * g|^2] = -\infty$.

A simple application of the Lebesque limit theorem gives $\lim_{T\to\infty} E[|\omega_T f|^2] = E[|f|^2]$. The functions

$$\theta_1(z) = |z|^2 \log^+ |z|, \qquad \theta_2(z) = |z|^2[-\log^- |z| + \tfrac{3}{2}]$$

are convex in the complex variable z. Since $\Omega_T(y) \geqq 0$ $(-\infty < y < \infty)$ and $\int_{-\infty}^{\infty} \Omega_T(y)\,dy = 1$, it follows that for $i = 1, 2$

$$\lim_{T\to\infty} \int_{-\infty}^{\infty} \theta_i[\Omega_T(y)*g(y)]\,dy = \int_{-\infty}^{\infty} \theta_i[g(y)]\,dy.$$

Since $E[|g|^2] = 2\int_{-\infty}^{\infty} \theta_1(g)\,dy - 2\int_{-\infty}^{\infty} \theta_2(g)\,dy + 3\|g\|^2$, we have

$$\lim_{T\to\infty} E[|\Omega_T(y)*g(y)|^2] = E[|g|^2].$$

The inequality (3) now follows from (9).

Let G be an arbitrary locally compact Abelian group with elements $x, y, \cdots$ and let $G^\wedge$ be its dual with elements $x^\wedge, y^\wedge, \cdots$. Let dx and $dx^\wedge$ be Haar measures on G and $G^\wedge$ so normalized that

$$\text{if } f^\wedge(x^\wedge) \sim \int_G f(x)\,\overline{(x, x^\wedge)}\,dx, \text{ then } f(x) \sim \int_{G^\wedge} f^\wedge(x^\wedge)\,(x, x^\wedge)\,dx^\wedge.$$

Under these assumptions Parseval's equality,

$$\|f(x)\|^2 = \int_G |f(x)|^2\,dx = \int_{G^\wedge} |f^\wedge(x^\wedge)|^2\,dx^\wedge = \|f^\wedge(x^\wedge)\|^2,$$

holds; see [3]. The argument leading to (3) can easily be extended to show that if $\|f\| = \|f^\wedge\| = 1$, then

$$E[|f|^2] + E[|f^\wedge|^2] \leqq 0, \tag{10}$$

where

$$E[|f|^2] = \int_G |f(x)|^2 \log |f(x)|^2\,dx,$$

$$E[|f^\wedge|^2] = \int_{G^\wedge} |f^\wedge(x^\wedge)|^2 \log |f^\wedge(x^\wedge)|^2\,dx^\wedge.$$

In particular if $f(\theta) \sim \sum_{-\infty}^{\infty} a_n e^{2\pi i n\theta}$, $a_n = \int_0^1 f(\theta) e^{-2\pi i n\theta}\, d\theta$, and

$$\sum_{-\infty}^{\infty} |a_n|^2 = \int_0^1 |f(\theta)|^2\, d\theta = 1,$$

then

$$\sum_{-\infty}^{\infty} |a_n|^2 \log |a_n|^2 + \int_0^1 |f(\theta)|^2 \log |f(\theta)|^2\, d\theta \leqq 0. \tag{11}$$

If $f(\theta) = 1$, so that $a_0 = 1$, $a_n = 0$ for $n \neq 0$, then equality obtains in (11); consequently the number 0 on the right hand side of (11) cannot be replaced by a smaller value. This also shows that (10) cannot be improved for the class of "all" locally compact Abelian groups. However it is conceivable that for individual groups the right hand side of (10) can be replaced by a smaller value. In particular this would seem to be the case when G is the real line which is the case we have treated in detail.

WASHINGTON UNIVERSITY.

REFERENCES.

[1] W. H. Fuchs, "On the magnitude of Fourier transforms," *Proc. Inter. Congress of Mathematicians at Amsterdam*, 1954, vol. 2, pp. 106-107.

[2] C. Shannon and W. Weaver, *A Mathematical Theory of Communication*, Urbana, 1949.

[3] A. Weil, *Intégration dans les groupes topologiques et ses applications*, Paris, 1940.

[4] H. Weyl, *Group Theory and Quantum Mechanics* (English translation), New York, 1931.

[5] A. Zygmund, *Trigonometrical Series*, Lwów, 1935.

INTEGRAL EQUIVALENCE OF QUADRATIC FORMS IN RAMIFIED LOCAL FIELDS.*

By O. T. O'Meara.

Two quadratic forms with associated matrices F and G are said to be integrally equivalent if there exists a unimodular matrix X such that $X^T FX = G$. Is it possible to attach a set of invariants to F which will completely characterize the equivalence class F, i.e., such that F and G will be integrally equivalent if and only if they have the same invariants? An answer to this problem has been given by Durfee [DI] in the case where the coefficients are taken in a local field in which 2 is a unit; Jones [JI] and Pall [PI] have established similar results over the 2-adic numbers. In an earlier paper [OI] I provided a characterization that holds for any local field in which 2 is a prime, and I discussed the equivalence of unitary forms in the ramified extensions of the 2-adic numbers. It is the purpose of this paper to solve the remaining case in the local theory—the equivalence of forms with coefficients in a field in which 2 is not a unit.

We shall consistently use the language of vector spaces and lattices when framing definitions and proving theorems. The invariants will be given in terms of fundamental invariants a_j, $v(j)$ which describe the numbers represented by certain invariant substructures of a given lattice. Using these quantities, the equivalence class of a lattice will be determined by Hasse symbols and quadratic residues.

Proofs will be based on the results of [OI], and no attempt will be made to give a self-contained discussion here. However, using the principles of the present paper it is possible to improve some of the earlier proofs and I have thought it worth while to include a simplified treatment of the invariance of type. Theorem 5.2 of [OII] will also be proved agan; but for this result, the present paper is independent of [OII].

I want to express my appreciation and indebtedness to Professor G. Whaples for making several valuable suggestions that have simplified the presentation of these results.

Notation. We preserve the notation used in [OI]. Thus our coefficient field F will be a local field [AI] with ring of integers $\mathfrak{o}$; π will denote a

* Received September 26, 1955; revised August 22, 1956.

prime element in F; throughout this paper we will assume that the residue class field is perfect, thought not necessarily finite, and that $\infty > e = \operatorname{ord} 2 \geqq 1$. We will continue to use the following notation: $a\pi^t$ will sometimes be written $[\pi^t]$ if a is a unit and $\{\pi^t\}$ is a is an integer. The relation $\alpha \cong \beta$ means that there is a unit in F whose square is α/β. If ϵ is a unit, then $\epsilon \cong 1 \bmod \pi$ follows immediately from the perfectness of the residue class field. Consider the greatest value of k for which $\epsilon \cong 1 + [\pi^k]$. If $k > 2e$, then $k = \infty$ by Hensel's lemma. On the other hand, we can again use the perfectness of the residue class field to prove that

$$(1) \qquad k < 2e \implies k \text{ odd}.$$

We define $\mathfrak{g}(\epsilon)$ as the ideal $\pi^k\mathfrak{o} + 2\mathfrak{o}$ where k is the maximal value just mentioned. For any $\epsilon\pi^r \in F$ we put

$$(2) \quad \mathfrak{g}(\epsilon\pi^r) = \mathfrak{g}(\epsilon) = \pi^k\mathfrak{o} + 2\mathfrak{o} \text{ if } r \text{ is even, } \mathfrak{g}(\epsilon\pi^r) = \mathfrak{o} \text{ if } r \text{ is odd, } \mathfrak{g}(0) = 0.$$

V will denote an n-dimensional vector space over F, provided with scalar product $x \cdot y$. It is assumed that V is non-degenerate, in other words

$$x \cdot y = 0 \text{ for all } y \in V \implies x = 0.$$

By a lattice L on V we mean an $\mathfrak{o}$-module $L \subseteq V$ which contains n independent vectors and is such that if the variable vector $x \in L$ is expressed in a fixed basis for V, then the coordinates of x in this basis have bounded denominators. It is well-known that a minimal basis $\langle x \rangle$ can be found such that $L = \sum \mathfrak{o}x_\lambda$. For a proof see Satz 1 [AsI]. Using this minimal basis it is easy to see that corresponding to any $x \in V$, there exists an $\alpha \in F$ such that $\alpha x \in L$, $\alpha\pi^{-1}x \notin L$; if $x \notin L$, then α must be in $\pi\mathfrak{o}$; otherwise $|\alpha| \geqq 1$. We shall refer to a subset $L' \subseteq V$ as a lattice in V if L' is a lattice on its containing space FL'.

Now let L and K be two lattices on V and suppose that they are expressed in the bases $L = \sum \mathfrak{o}x_\lambda$ and $K = \sum \mathfrak{o}y_\lambda$ respectively. We have seen in [Ol] that L is isometric to K (written $L \cong K$) if and only if the matrices $(x_i \cdot x_j)$ and $(y_i \cdot y_j)$ are integrally equivalent. If l is the quadratic form associated with $(x_i \cdot x_j)$, we write $L \cong (x_i \cdot x_j) \cong l$. We recall that $N(L) = \sum \mathfrak{o}x^2$ where x runs through L; and $d(L) = \det(x_i \cdot x_j)$. Then the assumption that V is non-degenrate is equivalent to $d(L) \neq 0$.

We will write $x \cdot L$ to denote $\{(x \cdot y) \mid y \in L\}$, where x is an arbitrary vector in V. More generally, we put

$$L \cdot K = \{(x \cdot y) \mid x \in L, y \in K\},$$

for any lattices L and K in V. It is easy to see that $x \cdot L$ is an $\mathfrak{o}$-ideal in F. This is also true for $L \cdot K$. For let $\langle z \rangle$ be an orthogonal basis for V. Since the elements of L and K have bounded denominators in $\langle z \rangle$, we can suppose that $L \subseteq \sum \mathfrak{o} z_\lambda$ and $K \subseteq \sum \mathfrak{o} z_\lambda$. Hence $L \cdot K$ generates a finite ideal $\pi^k \mathfrak{o}$, say. Suppose that $| x_0 \cdot y_0 | = | \pi^k |$. Then $\mathfrak{o} x_0 \cdot y_0 = \pi^k \mathfrak{o}$. Hence $L \cdot K = \pi^k \mathfrak{o}$. And so $L \cdot K$ is an $\mathfrak{o}$-ideal in F. The lattice L is said to be integral if $N(L) \subseteq \mathfrak{o}$; it is said to be totally integral if $L \cdot L \subseteq \mathfrak{o}$. Note that $N(L) \subseteq L \cdot L \subseteq \frac{1}{2} N(L)$.

By $a \circ L$ we will mean the lattice L on the same vector space V, but provided with the new metric $x \circ y = a(x \cdot y)$. This is not to be confused with the lattice aL which consists of the set of vectors az in the same space V provided with the same metric $x \cdot y$, where $z \in L$. But we have $a^2 \circ L \cong aL$.

The lattice J will be called a component of L if there exists a lattice K such that $L = J \oplus K$; K is then called the orthogonal complement of J in L.

A lattice L in V will be called π^i-unitary, or simply *unitary*, if

$$x \in L, x \notin \pi L \implies x \cdot L = \pi^i \mathfrak{o};$$

we call a unitary lattice L *proper* if $N(L) = L \cdot L$, otherwise *improper*. Note that if L is π^i-unitary in V, then $x \cdot L \subseteq \pi^i \mathfrak{o}$ whenever $x \in L$. And we also have

$$x \in FL, x \notin L \implies | x \cdot L | > | \pi^i | ; \tag{3}$$

for we can choose $\alpha \in \pi \mathfrak{o}$ such that $\alpha x \in L$, $\alpha x \notin \pi L$, and so $| x \cdot L | > | \pi^i |$. It is easy to see that any component of a π^i-unitary lattice is itself π^i-unitary; and conversely, the orthogonal sum of two π^i-unitary lattices is π^i-unitary. It is obvious that if L is π^i-unitary, then $\pi^\lambda \circ L$ is $\pi^{i+\lambda}$-unitary. We shall see later that L is π^0-unitary if and only if it is totally integral with determinant a unit.

1. The simplest invariant substructures. Let us consider a lattice L on V.

DEFINITION 1. *If i is a positive or negative integer, we call*

$$L_{(i)} = \{ x \mid x \in L \text{ and } x \cdot L \subseteq \pi^i \mathfrak{o} \}$$

the i-th invariant substructure of L.

The $\mathfrak{o}$-module $L_{(i)}$ defined in this way is a lattice on V; it is n-dimensional since

$$\pi^i (L \cdot L)^{-1} L \subseteq L_{(i)} \subseteq L.$$

By way of example we see that L is totally integral if and only if $L = L_{(0)}$; and $(\pi^{\lambda} \circ L)_{(\lambda+i)} = \pi^{\lambda} \circ L_{(i)}$. Note that

$$(4) \qquad \pi^{j-i} L_{(i)} \subseteq L_{(j)} \subseteq L_{(i)} \qquad \text{if } i \leqq j.$$

PROPOSITION 1. *If J is a π^i-unitary sublattice of L, then J is a component of L if and only if $J \subseteq L_{(i)}$.*

Proof. We need only prove the sufficiency. We can take $i = 0$. The vector space FJ being non-degenerate, we have $V = FJ \oplus (FJ)^{\perp}$ by Satz 1 of [WI]. Put $K = (FJ)^{\perp} \cap L$. Then K is a lattice on $(FJ)^{\perp}$. Now any $x \in L$ can be written uniquely in the form $w + z$ with $w \in FJ$ and $z \in (FJ)^{\perp}$. If $w \notin J$, then $|w \cdot J| > 1$ since J is unitary. Hence $|x \cdot J| > 1$, and this is impossible since $J \subseteq L_{(0)}$. Hence $w \in J$, and so $z \in K$. This proves the proposition.

It follows immediately from this proposition that every lattice L is an orthogonal sum of 1- or 2-dimensional unitary lattices. To see this we put $(x \cdot y)\mathfrak{o} = L \cdot L = \pi^k \mathfrak{o}$ where $x \in L$, $y \in L$; then if $x^2 \mathfrak{o} = \pi^k \mathfrak{o}$, $\mathfrak{o}x$ will be a π^k-unitary lattice in $L = L_{(k)}$, hence a component of L; otherwise $|x^2| < |\pi^k|$, say; then $\mathfrak{o}x + \mathfrak{o}y$ is π^k-unitary, hence a component of L. Induction completes the proof. By regrouping these components we get the result of Section 2 [OI], that every lattice L has a *canonical decomposition* $L = L_1 \oplus \cdots \oplus L_t$, where the components L_λ are $\pi^{s(\lambda)}$-unitary with $s(1) < s(2) < \cdots < s(t)$.

Now let L be a totally integral lattice with determinant a unit. If we express L as a canonical decomposition $L = \sum L_\lambda$ we must have $s(1) \geqq 0$; since $d(L)$ is a unit, it follows that $s(1) = 0$ and $t = 1$. Conversely, let L be a π^0-unitary lattice; then L is certainly totally integral. Express L as an orthogonal sum of 1- or 2-dimensional lattices. We can suppose that all 2-dimensional components have norms in $\pi\mathfrak{o}$. Hence $d(L)$ is a unit. We have therefore proved that *L is a π^0-unitary lattice if and only if L is totally integral with determinant a unit.*

Consider the canonical decomposition $L = \sum L_\lambda$. We contend that

$$(5) \qquad L_{(i)} = \sum_{1}^{j} \pi^{i-s(\lambda)} L_\lambda \oplus \sum_{j+1}^{t} L_\lambda$$

where j is such that $s(j) \leqq i < s(j+1)$. To prove this we write K for the right hand side of (5). If $\lambda \geqq j+1$, then $L_\lambda \cdot L = \pi^{s(\lambda)}\mathfrak{o} \subseteq \pi^{s(j+1)}\mathfrak{o} \subseteq \pi^i \mathfrak{o}$, and so $L_\lambda \subseteq L_{(i)}$; if $\lambda \leqq j$, then $(\pi^{i-s(\lambda)} L_\lambda) \cdot L_\lambda = \pi^i \mathfrak{o}$ and so $\pi^{i-s(\lambda)} L_\lambda \subseteq L_{(i)}$. Hence $K \subseteq L_{(i)}$. On the other hand, if $x \in L_{(i)}$ we have $x = \sum x_\lambda$ with $x_\lambda \in L_\lambda$;

then $x_\lambda \cdot L_\lambda \subseteq \pi^i\mathfrak{o}$ and so $x_\lambda \in \pi^{i-s(\lambda)}L_\lambda$ when $\lambda \leqq j$. Hence $L_{(i)} \subseteq K$. This proves the contention. In particular,

$$L_{(s(i))} = \sum_{1}^{i} \pi^{s(i)-s(\lambda)}L_\lambda \oplus \sum_{i+1}^{t} L_\lambda. \tag{6}$$

We see that $\pi^{s(i)-s(\lambda)}L_\lambda$ is now a $\pi^{2s(i)-s(\lambda)}$-unitary lattice; thus L_i is the first component in the canonical decomposition for $L_{(s(i))}$ that is induced by (6).

Consider another canonical decomposition $L = \sum K_\lambda$ for L in which K_λ is $\pi^{\sigma(\lambda)}$-unitary for $1 \leqq \lambda \leqq \tau$. Suppose no K_λ is $\pi^{s(i)}$-unitary for a certain fixed i $(1 \leqq i \leqq t)$. Then $L_{(s(i))}$ has the form (6); but we also have

$$L_{(s(i))} = \sum_{1}^{j} \pi^{s(i)-\sigma(\lambda)}K_\lambda \oplus \sum_{j+1}^{\tau} K_\lambda$$

where $\sigma(j) < s(i) < \sigma(j+1)$. Using the fact that $L_{(s(i))} \cdot L_{(s(i))} = \pi^{s(i)}\mathfrak{o}$, we see that this equation is impossible. Hence $t = \tau$ and $s(\lambda) = \sigma(\lambda)$ for $1 \leqq \lambda \leqq t$. We now show that $\dim L_i = \dim K_i$ and $N(L_i) \equiv N(K_i) \bmod \pi^{s(i)+1}$. By considering $L_{(s(i))}$ instead of L, we see that it suffices to consider the case $i = 1$, $s(1) = 0$. Since the first components are the only ones that can possibly represent units, it follow that $N(L_1) \equiv N(K_1) \bmod \pi$; in other words, L_1 is proper if and only if K_1 is proper. Now let M_1 denote the matrix of L in any basis corresponding to $\sum L_\lambda$; let M_2 correspond to the decomposition $\sum K_\lambda$. If $\bar{M}_1$ denotes the matrix M_1 when read in the residue class field, we see that there exists a non-singular matrix $\bar{X}$ such that $\bar{X}^T\bar{M}_1\bar{X} = \bar{M}_2$, since M_1 and M_2 are integrally equivalent. But rank $\bar{M}_1 = \dim L_1$. And similarly with M_2. Hence $\dim L_1 = \dim K_1$. We therefore see that for two decompositions $\sum L_\lambda$ and $\sum K_\lambda$ we have

$$s(\lambda) = \sigma(\lambda), \quad \dim L_\lambda = \dim K_\lambda, \quad L_\lambda \text{ proper} \Leftrightarrow K_\lambda \text{ proper},$$

for $1 \leqq \lambda \leqq t = \tau$. Thus we have proved Theorem 3.1 of [OI] without computation. Any two lattices $L = \sum L_\lambda$ and $K = \sum K_\lambda$ which satisfy these equations are said to be *of the same type.*

DEFINITION 2. *Put* $\pi^{u(i)}\mathfrak{o} = N(L_{(s(i))})$ *for* $1 \leqq \lambda \leqq t$.

Immediately we see that

$$|\, 2\pi^{s(i)} \,| \leqq |\, \pi^{u(i)} \,| \leqq |\, \pi^{s(i)} \,|; \tag{7}$$

while if $\sum L_\lambda$ is a canonical decomposition of L we must have

$$N(L_i) \subseteq \pi^{u(i)}\mathfrak{o}. \tag{8}$$

If $\dim L_i$ is odd, L_i has at least one 1-dimensional component and so L_i is proper. In this case $N(L_i)=\pi^{s(i)}\mathfrak{o}=\pi^{u(i)}\mathfrak{o}$.

DEFINITION 3. *If $L=\sum L_\lambda$ is a canonical decomposition of L, put*

$$\mathfrak{R}L=\pi^{-s(t)}L_{(s(t))}=\pi^{-s(t)}L_t\oplus\cdots\oplus\pi^{-s(1)}L_1;$$

and when $s(i+1)=0$, put

$$\mathfrak{P}L=L_{(0)}=\pi^{-s(1)}L_1\oplus\cdots\oplus\pi^{-s(i)}L_i\oplus L_{i+1}\oplus\cdots\oplus L_t.$$

We see that the decomposition for $\mathfrak{P}L$ in this definition may cease to be canonical. Note that $\mathfrak{R}\mathfrak{R}L=L$ and $\mathfrak{P}\mathfrak{P}L=\mathfrak{P}L$. If $s(1)=0$, then $\mathfrak{P}L=L$; if $s(t)=0$, then $\mathfrak{P}L=\mathfrak{R}L$.

We know that $N(L_i)\subseteq\pi^{u(i)}\mathfrak{o}$. Can $N(L_i)=\pi^{u(i)}\mathfrak{o}$ ever be attained by a canonical decomposition $L=\sum L_\lambda$? We shall show more than this. In fact, we shall exhibit a saturated decomposition $L=\sum J_\lambda$ for L in which $N(J_\lambda)=\pi^{u(\lambda)}\mathfrak{o}$ for all λ $(1\leqq\lambda\leqq t)$.

DEFINITION 4. *The component L_j of the canonical decomposition $L=\sum L_\lambda$ is said to be saturated if $u(j)=\operatorname{ord}N(L_j)$; the decomposition $\sum L_\lambda$ is called saturated if all its components are saturated.*

PROPOSITION 2. *L has a saturated decomposition.*

Proof. Let $L=\sum L_\lambda$ be a canonical decomposition such that $N(L_\lambda)=\pi^{u(\lambda)}\mathfrak{o}$ for $\lambda=1,2,\cdots,j-1$ where $1\leqq j\leqq t$. We must extend this property to $\lambda=j$. We can assume that $s(j)=0$. If $N(L_j\oplus\cdots\oplus L_t)=\pi^{u(j)}\mathfrak{o}$, we can take a canonical decomposition $J_j\oplus\cdots\oplus J_t$ for $L_j\oplus\cdots\oplus L_t$ in which $N(J_j)=\pi^{u(j)}\mathfrak{o}$, and we are through. Now assume that $|N(L_j\oplus\cdots\oplus L_t)|<|\pi^{u(j)}|$. Then by (6) there exists a $k<j$ such that $N(\mathfrak{R}L_k)=N(\pi^{-s(k)}L_k)=\pi^{u(j)}\mathfrak{o}=\pi^{u(k)-2s(k)}\mathfrak{o}$.

Consider $\mathfrak{R}L=\cdots\oplus L_j\oplus\cdots\oplus\mathfrak{R}L_k\oplus\cdots$. Then

$$L_j\oplus\mathfrak{R}L_k=L_j\oplus\pi^{-s(k)}L_k=J_j\oplus J_k$$

with $N(J_j)=\pi^{u(j)}\mathfrak{o}$, since $\mathfrak{R}L_k$ has norm $\pi^{u(j)}\mathfrak{o}$. We then have $L_k\oplus L_j=\mathfrak{R}J_k\oplus J_j$, where J_j has the required norm, while $\mathfrak{R}J_k$ continues to have norm $\pi^{u(k)}\mathfrak{o}$ since

$$|N(J_j)|=|\pi^{u(j)}|=|\pi^{u(k)-2s(k)}|<|N(L_k\oplus L_j)|=|N(\mathfrak{R}J_k\oplus J_j)|.$$

Then $L=\sum_{\lambda\neq j,k}L_\lambda\oplus\mathfrak{R}J_k\oplus J_j$ is a canonical decomposition which extends the required property to j. Repeating this to $\lambda=t$ proves the result.

COROLLARY 2. *L_j is a saturated component of $L = \sum L_\lambda$ if and only if $\mathfrak{R} L_j$ is a saturated component of $\mathfrak{R} L = \sum \mathfrak{R} L_\lambda$.*

Proof. Suppose that L_j is saturated, but that $\mathfrak{R} L_j$ is not. Let $L = \sum K_\lambda$ be such that $\mathfrak{R} K_j$ is saturated in $\sum \mathfrak{R} K_\lambda$. Then $|N(\mathfrak{R} K_j)| > |N(\mathfrak{R} L_j)|$, and so $|N(K_j)| > |N(L_j)|$, which is impossible. On the other hand, if $\mathfrak{R} L_j$ is saturated, then so is $\mathfrak{R}\mathfrak{R} L_j = L_j$. q. e. d.

From this follows

$$u_L(j) = 2s(j) + u_{\mathfrak{R}L}(t - j + 1). \tag{9}$$

And relation (4) implies

$$|\pi^{u(i)}| \geqq |\pi^{u(j)}|, \qquad |\pi^{u(j)-2s(j)}| \geqq |\pi^{u(i)-2s(i)}| \qquad \text{if } i \leqq j. \tag{10}$$

2. Canonical bases. We have seen that any lattice L can be decomposed into an orthogonal sum of 1- and 2-dimensional unitary lattices. By choosing a basis for each of these components we can induce a minimal basis on L. Call this basis $\langle x \rangle$ and put $t(\lambda) = \operatorname{ord} x_\lambda \cdot L$; suppose that $t(1) \leqq t(2) \leqq \cdots \leqq t(n)$. Then the basis obtained in this way is said to be *semi-canonical.* If we group vectors, we get a corresponding canonical decomposition for L, and so the quantities $t(\lambda)$ are independent of $\langle x \rangle$. Thus x_λ will either be orthogonal to all the other basis vectors, and $\mathfrak{o} x_\lambda$ will then be $\pi^{t(\lambda)}$-unitary; or there is precisely one basis vector $x_{\lambda-1}$, say, which is not orthogonal to x_λ, and then $t(\lambda) = t(\lambda - 1)$ with $\mathfrak{o} x_{\lambda-1} + \mathfrak{o} x_\lambda$ unitary.

Consider the semi-canonical basis $\langle x \rangle$ for L. Generalizing a certain change of basis used in [OI], [OII], we introduce a transformation which will be denoted by the symbol $\operatorname{op}(x_i \to x_i + \alpha x_j)$. Let x_{i-1} denote that vector (if any) which is not orthogonal to x_i; let x_{j+1} denote that vector (if any) which is not orthogonal to x_j. We assume that

$$\alpha \in \mathfrak{o}, \qquad t(j) \geqq t(i), \qquad i \neq j, \qquad x_i \cdot x_j = 0.$$

Suppose that we write $\operatorname{op} x_i = x_i + \alpha x_j$. We make the further assumption that $\mathfrak{o}(\operatorname{op} x_i)$, respectively $(\mathfrak{o} x_{i-1} + \mathfrak{o}(\operatorname{op} x_i))$, are still $\pi^{t(i)}$-unitary; in other words, we assume that

$$|(\operatorname{op} x_i)^2| = |\pi^{t(i)}|, \qquad |(\operatorname{op} x_i)^2 (x_{i-1})^2 - (x_{i-1} \cdot x_i)^2| = |\pi^{2t(i)}|,$$

respectively. The transformation then consists in replacing x_i by the basis

vector $\operatorname{op} x_i = x_i + \alpha x_j$ and leaving all other basis elements fixed, with the exception of x_j and (possibly) x_{j+1} which are defined in the following way:

$$\operatorname{op} x_j = x_j + A(\operatorname{op} x_i) + Bx_{i-1}, \quad \operatorname{op} x_{j+1} = x_{j+1} + A'(\operatorname{op} x_i) + B'x_{i-1}, \tag{11}$$

where, if $x_i \cdot x_{i-1} = 0$,

$$A = -\alpha x_j^2/(\operatorname{op} x_i)^2, \quad A' = -\alpha(x_j \cdot x_{j+1})/(\operatorname{op} x_i)^2, \quad B = 0 = B', \tag{11a}$$

and, if $x_i \cdot x_{i-1} \neq 0$,

$$\begin{aligned} A &= -\alpha x_j^2 x_{i-1}^2/D, & A' &= -\alpha(x_j \cdot x_{j+1}) x_{i-1}^2/D, \\ B &= \alpha x_j^2 (x_i \cdot x_{i-1})/D, & B' &= \alpha(x_j \cdot x_{j+1})(x_i \cdot x_{i-1})/D \end{aligned} \tag{11b}$$

where $D = (\operatorname{op} x_i)^2 (x_{i-1})^2 - (x_i \cdot x_{i-1})^2$. By inspection, A, B, A', B', are all integers. Hence in (11b) we have

$$(\mathfrak{o}x_{i-1} + \mathfrak{o}x_i) \oplus \mathfrak{o}x_j = (\mathfrak{o}x_{i-1} + \mathfrak{o}(\operatorname{op} x_i)) \oplus (\mathfrak{o}(\operatorname{op} x_j))$$

or

$$(\mathfrak{o}x_{i-1} + \mathfrak{o}x_i) \oplus (\mathfrak{o}x_j + \mathfrak{o}x_{j+1}) = (\mathfrak{o}x_{i-1} + \mathfrak{o}(\operatorname{op} x_i)) \oplus (\mathfrak{o}(\operatorname{op} x_j) + \mathfrak{o}(\operatorname{op} x_{j+1}));$$

and similar equations hold for (11a). We see that the resulting basis for L is still semi-canonical. This is the transformation indicated by $\operatorname{op}(x_i \to x_i + \alpha x_j)$. We call the new basis $\langle \operatorname{op} x \rangle$.

As a simple example on the use of these transformations we see that any semi-canonical basis for a unitary lattice can be refined to a *canonical* basis ([OI], Definition 2.1). This can be done with each component of a general lattice; every lattice must therefore have a canonical basis ([OI], Theorem 2.4).

Using these transformations it is possible to find a special kind of basis for a π^0-unitary lattice. Let $\pi^u \mathfrak{o} = N(L)$, and put $\pi^v \mathfrak{o} = \sum x^2 \mathfrak{o} + 2\mathfrak{o}$ with $x \in L$, $u + \operatorname{ord} x^2$ odd. Then there is a decomposition

$$L = L_1 \oplus L_2 \oplus \sum H_\lambda \tag{12}$$

and a unit ϵ, such that

$$L_1 \cong \epsilon \text{ if } \dim L \text{ is odd}, \quad L_1 \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \{\pi^v\} \end{pmatrix} \text{ if } \dim L \text{ is even}, \tag{13}$$

$$L_2 \cong \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix}, \quad H_\lambda \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{14}$$

We have discussed these decompositions in Sections 14, 17, 18 of [OI] and proofs are omitted here.

3. On cancelling hyperbolic planes. We call a lattice a *π^i-hyperbolic plane* if its associated matrix is of the form $\begin{pmatrix} 0 & \pi^i \\ \pi^i & 0 \end{pmatrix}$; a unit **hyperbolic** plane has $i = 0$. We have seen in [OII] that if $H_1 \oplus L_1 \cong H_2 \oplus L_2$ with $H_1 \cong H_2$ hyperbolic planes, then $L_1 \cong L_2$; this is the local integral analogue of Witt's theorem [WI]. In discussing the invariants of a given lattice we are therefore free to adjoin as many hyperbolic planes as we please. We say that the j-th component of a canonical decomposition $\sum L_\lambda$ is *big* if $\dim L_j \geqq 9$. The decomposition $\sum L_\lambda$ is called big if $\dim L_\lambda \geqq 9$ for $1 \leqq \lambda \leqq t$.

We now give a simple proof of Theorem 5.2 [OII].

PROPOSITION 3. *$H_1 \oplus L_1 = L = H_2 \oplus L_2$ are two decompositions of L, where H_1 and H_2 are isometric hyperbolic planes. Then $L_1 \cong L_2$.*

Proof. Write $H_1 = \mathfrak{o}x_1 + \mathfrak{o}y_1$, $H_2 = \mathfrak{o}x_2 + \mathfrak{o}y_2$, with $x_1{}^2 = y_1{}^2 = x_2{}^2 = y_2{}^2 = 0$. We can assume that $x_1 \cdot y_1$ and $x_2 \cdot y_2$ are units. Then $H_1 \subseteq L_{(0)}$ and $H_2 \subseteq L_{(0)}$.

Case 1. $H_1 \cdot H_2 = \mathfrak{o}$. We can suppose that $x_1 \cdot y_2$ is a unit; hence $(\mathfrak{o}x_1 + \mathfrak{o}y_2)$ is a component of L by Proposition 1. Writing

$$L = (\mathfrak{o}x_1 + \mathfrak{o}y_1) \oplus L_1 = (\mathfrak{o}x_1 + \mathfrak{o}y_2) \oplus L_1' = (\mathfrak{o}x_2 + \mathfrak{o}y_2) \oplus L_2,$$

we see that it suffices to prove this case for $x_1 = x_2$, $y_1 \neq y_2$. Then

$$L = (\mathfrak{o}x_1 + \mathfrak{o}y_1) \oplus \sum \mathfrak{o}z_\lambda = (\mathfrak{o}x_1 + \mathfrak{o}y_2) + \sum \mathfrak{o}z_\lambda = (\mathfrak{o}x_1 + \mathfrak{o}y_2) \oplus \sum \mathfrak{o}w_\lambda$$

where $w_\lambda = z_\lambda - (y_2 \cdot z_\lambda)(y_2 \cdot x_1)^{-1}x_1$. By inspection, $w_\lambda \cdot w_\mu = z_\lambda \cdot z_\mu$. Hence $L_1 \cong L_2$.

Case 2. $H_1 \cdot H_2 \subseteq \pi\mathfrak{o}$. Then $H_1 + H_2$ is π^0-unitary and so $H_1 + H_2$ is a component of L. It therefore suffices to prove the result for $L = H_1 + H_2$. Assume this is so. Then $N(L) = 2\mathfrak{o}$, hence $N(L_1) = N(L_2) = 2\mathfrak{o}$, hence L_1 and L_2 represent 2 since they are unitary. But $d(L_1) \cong d(L_2)$. Hence $L_1 \cong L_2$ by Theorem 14.3 of [OI]. This proves the proposition.

COROLLARY 3. *L and K are lattices of the same type such that $L_{(s(j))}$ and $K_{(s(j))}$ both represent the same number ϵ of ordinal $s(j)$. If $I \oplus L \cong J \oplus K$ where $I \cong \epsilon \cong J$, then $L \cong K$.*

Proof. We can take $s(j) = 0$, ϵ a unit. It suffices to prove $L \cong K$ for

$$I \cong J \cong \epsilon \oplus -\epsilon \cong \begin{pmatrix} -\epsilon & 1 \\ 1 & 0 \end{pmatrix},$$

instead of for the given I and J. In virtue of Proposition 1, we can write $I \oplus L = I \oplus L_1 \oplus L_2$ with $L_1 \cong \epsilon$. Now $I \oplus L_1 = H \oplus L_1' \cong H \oplus L_1$ where H is a unit hyperbolic plane. And similarly with K. Hence $H \oplus L \cong I \oplus L \cong J \oplus K \cong H' \oplus K$. Hence $L \cong K$ by Proposition 3. q.e.d.

4. Supersaturated decompositions. It is our intention here to show that the numbers represented by $L_{(s(j))}$ can be described in a simple way in terms of the quantities a_j and $v(j)$ defined below. We shall then show that any big lattice has a canonical decomposition in which the j-th component represents all numbers represented by the $s(j)$-th invariant substructure.

DEFINITION 5. *For each j $(1 \leqq j \leqq t)$, put $\pi^{v(j)}\mathfrak{o} = \sum \mathfrak{o}x^2 + 2\pi^{s(j)}\mathfrak{o}$ where x runs through all vectors in $L_{(s(j))}$ for which* $\operatorname{ord} x^2$ *and $u(j)$ have opposite parity.*

We immediately see that

$$u(j) \leqq v(j) \leqq e + s(j), \tag{15}$$

$$u(j) = v(j) \iff u(j) = e + s(j), \tag{16}$$

$$v(j) < e + s(j) \implies u(j) + v(j) \text{ odd}. \tag{17}$$

PROPOSITION 4. *There exists an a_j of ordinal $u(j)$ such that every number represented by $L_{(s(j))}$ is of the form $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$.*

Proof. Take $x_0 \in L_{(s(j))}$ of norm $\pi^{u(j)}\mathfrak{o}$ and define $a_j = x_0{}^2$. Suppose that $x \in L_{(s(j))}$ cannot be expressed in the required form. Then $|\pi^{v(j)}| < |x^2| \leqq |a_j|$ and so $u(j)$ and $\operatorname{ord} x^2$ must have the same parity. In virtue of the perfectness of the residue class field we can take $x^2 = \beta^2 a_j(1 + [\pi^\gamma])$ where $\beta \in \mathfrak{o}$ and $|\pi^\gamma| < 1$. Suppose that β and γ have been chosen so that γ is maximal for the given x. Then $|\pi^\gamma| > |2|$ since x^2 does not have the desired form. Hence γ is odd by (1). But $|(x + \beta x_0)^2| = |\beta^2 a_j \pi^\gamma| > |\pi^{v(j)}|$, and this is impossible by definition of $v(j)$. q.e.d.

From now on we shall understand by $a_j = a_j(L)$ a fixed element of F which describes $L_{(s(j))}$ according to Proposition 4. If $\bar{a}_j$ is used instead of a_j, then $a_j \cong \bar{a}_j \bmod \pi^{v(j)}$. Note that the elements of the form $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$ form an additive group in F. This follows from the relation

$$a_j\alpha_1{}^2 - a_j\alpha_2{}^2 \equiv a_j(\alpha_1 - \alpha_2)^2 \bmod \pi^{v(j)}.$$

We see that $\bar{a}_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o} = a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$ if $\bar{a}_j \cong a_j \bmod \pi^{v(j)}$. In particular, such an $\bar{a}_j$ can be used instead of a_j in Proposition 4. Consider the quantities

$s(j)$, $u(j)$, $v(j)$, a_j for L; if $S(j)$, $U(j)$, $V(j)$, A_j are the same quantities computed for $(\pi^k \circ L)$, then $S(j) = s(j) + k$ and so $(\pi^k \circ L)_{(S(j))} = \pi^k \circ L_{(s(j))}$; hence

$$U(j) = u(j) + k, \qquad V(j) = v(j) + k, \qquad A_j \cong a_j\pi^k \bmod \pi^{V(j)}.$$

DEFINITION 6. *We say that the component L_j of the canonical decomposition $\sum L_\lambda$ is supersaturated if L_j represents all numbers of the form $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$. The decomposition $\sum L_\lambda$ is called supersaturated if all its components are supersaturated.*

It follows from (6) that if a lattice has a supersaturated component L_j, then $L_{(s(j))}$ represents all numbers in the additive group $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$. In particular, L_j and $L_{(s(j))}$ then represent the same numbers. Clearly a supersaturated component must be saturated. We would like to proceed as we did with the saturated decompositions and we ask whether every lattice must have at least one supersaturated decomposition. In general the answer must be no: for what can be done with a 1-dimensional component? But the result is true for big lattices and we shall establish it after proving the next two propositions.

PROPOSITION 5. *If L is π^0-unitary and* $\dim L \geqq 5$, *then L represents every number of the form $a_1\mathfrak{o}^2 + \pi^{v(1)}\mathfrak{o}$.*

Proof. It suffices to prove the result for an a_1 that is actually represented by L. Select $x_1 \in L$ such that $x_1{}^2 = a_1$. It follows from (12) and (14) that there is a vector $x_2 \in L$ such that $x_2{}^2 = \pi^{v(1)}$. Now let α be a number of the form $a_1\mathfrak{o}^2 + \pi^{v(1)}\mathfrak{o}$. We must prove that L represents α. Suppose that L represents $\alpha + \epsilon\pi^\gamma$ where ϵ is a unit, but that L does not represent $\alpha + \{\pi^{\gamma+1}\}$. Then $|\pi^\gamma| \leqq |\pi^{v(1)}|$.

(i) Let $|\pi^\gamma| > |2|$. Then $u(1)$ and $v(1)$ have opposite parity. Suppose that $z^2 = \alpha + \epsilon\pi^\gamma$. If γ and $v(1)$ are of the same parity, then by the perfectness of the residue class field there is a $\beta \in \mathfrak{o}$ such that $(z + \beta x_2)^2 \equiv \alpha \bmod \pi^{\gamma+1}$, and this is impossible by definition of γ. Hence $\gamma + u(1)$ is even. Using x_1 instead of x_2 shows that this is impossible. Hence (ii) let $|\pi^\gamma| \leqq |2|$. Then we write $L = H \oplus K$ where H is a hyperbolic plane, and we see that K must represent $\alpha + \epsilon\pi^\gamma \bmod 2$. Select $w \in K$ such that $w^2 = \alpha + 2\delta\pi^\Gamma$, and then $y \in H$ such that $y^2 = -2\delta\pi^\Gamma$. We see that $w + y$ is the vector required. This proves the proposition.

PROPOSITION 6. *L is a big π^0-unitary lattice and α is represented by L. Then there is a decomposition $L = L_1 \oplus L_2$ where L_2 represents the same numbers as L, and* $L_1 \cong \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$.

Proof. Write $L = H \oplus K$ where H is a hyperbolic plane. Then $u_K(1) = u_L(1)$ and $v_K(1) = v_L(1)$, so that L and K represent the same numbers by Propositions 4 and 5. It is easily seen that corresponding to this decomposition we can write

$$H \oplus K \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots.$$

Call the corresponding basis $x_1, x_2, x_3, \cdots$ and apply $\mathrm{op}(x_1 \to x_1 + x_3)$. Using equations (11) and (11b) this gives $H \oplus K = H' \oplus K'$ with $H' \cong \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$, and it follows by inspection that $K \cong K'$. Hence $L = H' \oplus K'$ is the required decomposition. This proves the proposition.

PROPOSITION 7. *If L is big, it has a supersaturated decomposition.*

Proof. Suppose that we have found a saturated decomposition $L = \sum K_\lambda$ such that the components K_λ are supersaturated for $\lambda = 1, 2, \cdots, j-1$ where $1 \leqq j \leqq t$. We must extend this property to $\lambda = j$. We can take $s(j) = 0$ and $|\pi^{v(j)}| > |2|$. Then for each λ $(1 \leqq \lambda \leqq t)$ there is an α_λ represented by K_λ such that

$$|\pi^{-2s(1)}\alpha_1 + \cdots + \pi^{-2s(j-1)}\alpha_{j-1} + \alpha_j + \cdots + \alpha_t| = |\pi^{v(j)}|.$$

since $L_{(s(j))}$ represents $[\pi^{v(j)}]$. By Proposition 6, write $K_\lambda = (\mathfrak{o}x_\lambda + \mathfrak{o}y_\lambda) \oplus K_\lambda{}^*$ where $K_\lambda{}^*$ represents the same numbers as K_λ, and $x_\lambda{}^2 = \alpha_\lambda$, $y_\lambda{}^2 = 0$. Then

$$x = \pi^{-s(1)}x_1 + \cdots + \pi^{-s(j-1)}x_{j-1} + x_j + \cdots + x_t$$

is in $L_{(s(j))}$ and $(\mathfrak{o}x + \mathfrak{o}y_j)$ is unitary. Hence $(\mathfrak{o}x + \mathfrak{o}y_j)$ is a component for the lattice $\sum(\mathfrak{o}x_\lambda + \mathfrak{o}y_\lambda)$. This yields a new saturated decomposition $L = \sum J_\lambda$ in which the J_λ are still supersaturated when $1 \leqq \lambda \leqq j-1$, while J_j now represents a number of ordinal $v(j)$ and is therefore supersaturated in virtue of Proposition 5. Thus we have extended our result to $\lambda = j$. Proceeding to $\lambda = t$ proves the result.

COROLLARY 7. *L_j is a supersaturated component of the big lattice $L = \sum L_\lambda$ if and only if $\mathfrak{R} L_j$ is a supersaturated component of $\mathfrak{R} L = \sum \mathfrak{R} L_\lambda$.*

Proof. Similar to Corollary 2.

We remark that if we enlarge a given lattice by adjoining $\pi^{s(i)}$-hyperbolic planes, then the enlarged lattice has the same a's and v's as the original one. We can easily see that

$$v_L(j) = 2s(j) + v_{\mathfrak{R}L}(t-j+1) \tag{18}$$

holds for a big lattice. By the last remark it must therefore be true in general.

Let L^* denote a big lattice obtained by adjoining $\pi^{s(i)}$-hyperbolic planes to L. Associated with $L_{(s(j))}$ is the group $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$, and the same group is associated with $L_{(s(j))}{}^*$; we know that the elements of this group are precisely the numbers represented by $L_{(s(j))}{}^*$. By considering the relation

$$L_{(s(i))}{}^* \supseteq L_{(s(j))}{}^* \supseteq \pi^{s(j)-s(i)}L_{(s(i))}{}^*$$

we see that

$$a_i\mathfrak{o}^2 + \pi^{v(i)}\mathfrak{o} \supseteq a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o},\ \pi^{-2s(i)}(a_i\mathfrak{o}^2 + \pi^{v(i)}\mathfrak{o}) \subseteq \pi^{-2s(j)}(a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}) \tag{19}$$

holds for L if $i \leqq j$.

5. The ideal $\mathfrak{f}_j$. We now introduce $\mathfrak{f}_j$ for values of j in $1 \leqq j \leqq t-1$. This is an ideal defined in terms of the u's and v's in the following way:

(i) *if $u(j)$ and $u(j+1)$ have opposite parity, put* $\pi^{2s(j)}\mathfrak{f}_j = \pi^{u(j)+u(j+1)}\mathfrak{o}$;

(ii) *if $u(j)$ and $u(j+1)$ have the same parity, let $\pi^{2s(j)}\mathfrak{f}_j$ be the ideal generated by* $\pi^{u(j)+u(j+1)}\mathfrak{g}(a_ja_{j+1})$, $\pi^{u(j)+v(j+1)}$, $\pi^{u(j+1)+v(j)}$, $2\pi^{(u(j)+u(j+1))/2+s(j)}$.

We note that $\mathfrak{f}_j$ has the same value if we replace a_j, a_{j+1} by $a_j + \{\pi^{v(j)}\}$, $a_{j+1} + \{\pi^{v(j+1)}\}$, respectively. In other words, the representative of $a_j \bmod \pi^{v(j)}$ is immaterial. It is easily seen from (9) and (18) that $\mathfrak{f}_j(L) = \mathfrak{f}_{t-j}(\mathfrak{R}L)$; and $\mathfrak{f}_j(\alpha \circ L) = \mathfrak{f}_j(L)$. Since the u's, v's and a's are unaltered by the adjunction of $\pi^{s(i)}$-hyperbolic planes which leave the type unaltered, it follows that such an adjunction cannot alter the $\mathfrak{f}$'s. By considering a supersaturated decomposition of a big lattice, we see that for any L, $|\pi^{-u(j)}\mathfrak{f}_j| \leqq |\pi^{v(j)}|$ when $s(j) = 0$. Thus $\mathfrak{f}_j$ is always contained in $\pi\mathfrak{o}$. Note that if $L = \sum L_\lambda$ is supersaturated, then

$$\mathfrak{f}_j(L) = \mathfrak{f}_1(L_j \oplus L_{j+1}). \tag{20}$$

Let $\langle x \rangle$ denote a semi-canonical basis for L and put $t(\lambda) = \mathrm{ord}(x_\lambda \cdot L)$. Then we shall have occasion to use the relation

$$x_\lambda{}^2 x_\mu{}^2 \mathfrak{g}(x_\lambda{}^2 x_\mu{}^2) \subseteq \pi^{2t(\lambda)}\mathfrak{f}_j \tag{21}$$

where $x_\lambda \in L_1 \oplus \cdots \oplus L_j$, $x_\mu \in L_{j+1} \oplus \cdots \oplus L_t$. To prove the validity of this relation, we take $s(j) = 0$ and note that $\pi^{-t(\lambda)} x_\lambda \in L_{(s(j))}$, hence $\pi^{-2t(\lambda)} x_\lambda^2 = \alpha^2 a_j + \{\pi^{v(j)}\}$ with α an integer; similarly $x_\mu^2 = \beta^2 a_{j+1} + \{\pi^{v(j+1)}\}$. Hence (21) follows from the definition of $\mathfrak{f}_j$.

The u's and v's take on a simpler form when $s(j+1) = s(j) + 1$. For instance, it follows from (10) that

$$(22) \qquad |\pi^{u(j)+2}| \leqq |\pi^{u(j+1)}| \leqq |\pi^{u(j)}|.$$

So we find

$$(23) \qquad u(j+1) = u(j) \Longrightarrow \pi^{2s(j)}\mathfrak{f}_j = \pi^{u(j)+v(j)}\mathfrak{o},$$

$$(24) \quad u(j+1) = u(j) + 1 \Longrightarrow \pi^{2s(j)}\mathfrak{f}_j = \pi^{2u(j)+1}\mathfrak{o},$$

$$(25) \quad u(j+1) = u(j) + 2 \Longrightarrow \pi^{2s(j)}\mathfrak{f}_j = \pi^{u(j)+v(j+1)}\mathfrak{o} \text{ if } s(j+1) = s(j) + 1.$$

The result (23) follows by observing that we can take $a_j = a_{j+1}$, that $v(j+1) \geqq v(j)$, and that $|2\pi^{(u(j)+u(j+1))/2+s(j)}| \leqq |\pi^{u(j+1)+v(j)}|$. The result (24) is trivial. The result (25) follows by taking $a_{j+1} = a_j\pi^2$ and noting that $v(j) \leqq v(j+1) \leqq v(j) + 2$, $|2\pi^{(u(j)+u(j+1))/2+s(j)}| \leqq |\pi^{u(j)+v(j+1)}|$. It is clear from the proofs that (23) and (24) hold even if $s(j+1) \neq s(j) + 1$.

The next lemma will be used in proving the necessity of Theorem 2. We shall establish this lemma in full generality in Theorem 3.

LEMMA 1. *Let $L = \sum K_\lambda = \sum J_\lambda$ be two canonical decompositions of L such that $N(K_1) = \pi^{u(1)}\mathfrak{o} = N(J_1)$ and $s(1) = 0$, where* $\dim K_1 = \dim J_1$ *is even and $\geqq 4$. Then $K_1 \cong J_1$* $(\operatorname{mod} \mathfrak{f}_1\pi^{-u(1)})$ *and $d(K_1)/d(J_1) \cong 1$* $\operatorname{mod} \mathfrak{f}_1$.

Proof. We put $\mathfrak{b}_1 = \pi^{-u(1)}\mathfrak{f}_1$; then we have $\mathfrak{b}_1 = \pi^{u(2)}\mathfrak{o}$ if $u(1) + u(2)$ is odd; while if $u(1)$ and $u(2)$ have the same parity we have

$$\mathfrak{b}_1 = [\pi^{u(2)}\mathfrak{g}(a_1 a_2), \pi^{v(2)}, \pi^{u(2)-u(1)+v(1)}, 2\pi^{(u(2)-u(1))/2}].$$

Using equations (12)-(14) we can express $K_1 = H \oplus K_1^*$, $J_1 = H' \oplus J_1^*$ where K_1^* and J_1^* are 4-dimensional while $H \cong H'$ are orthogonal sums of hyperbolic planes. Since the orthogonal complements of H and H' in L are isometric, it follows that we can assume that K_1 and J_1 are 4-dimensional. Let a_1 denote a number of ordinal $u(1)$ that is represented by K_1.

If $u(2) = u(1)$, then $\mathfrak{b}_1 = \pi^{v(1)}\mathfrak{o}$ and so (12)-(14) imply that

$$K_1 \cong \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cong J_1 \operatorname{mod} \mathfrak{b}_1.$$

Hence we can assume that $u(2) > u(1)$. We do so from now on.

Write K_1 in a basis $(\mathfrak{o}y_1 + \mathfrak{o}y_2) \oplus (\mathfrak{o}y_3 + \mathfrak{o}y_4)$ in which

$$K_1 \cong \begin{pmatrix} \epsilon\pi^{u(1)} & 1 \\ 1 & \alpha\pi^{v(1)} \end{pmatrix} \oplus \begin{pmatrix} \delta\pi^{u(1)} & 1 \\ 1 & \beta\pi^{v(1)} \end{pmatrix}$$

where ϵ and δ are units and where α and β are integers. Then there exist vectors x_1 and x_2 in J_1, X_1 and X_2 in $J = J_2 \oplus \cdots \oplus J_t$, such that

$$y_1 = x_1 + X_1, \qquad y_2 = x_2 + X_2.$$

It is easily seen that $\mathfrak{o}x_1 + \mathfrak{o}x_2$ is unitary and we write

$$L = (\mathfrak{o}x_1 + \mathfrak{o}x_2) \oplus (\mathfrak{o}\bar{x}_3 + \mathfrak{o}\bar{x}_4) \oplus J = (\mathfrak{o}y_1 + \mathfrak{o}y_2) \oplus (\mathfrak{o}\bar{x}_3 + \mathfrak{o}\bar{x}_4) \oplus J^*.$$

If K denotes the orthogonal complement of K_1 in L, we have

$$(\mathfrak{o}\bar{x}_3 + \mathfrak{o}\bar{x}_4) \oplus J^* = (\mathfrak{o}y_3 + \mathfrak{o}y_4) \oplus K.$$

Hence $y_3 = z_3 + Z_3$, $y_4 = z_4 + Z_4$, with z_3 and z_4 in $(\mathfrak{o}\bar{x}_3 + \mathfrak{o}\bar{x}_4)$, and Z_3 and Z_4 in J^*. Again we see that $\mathfrak{o}z_3 + \mathfrak{o}z_4$ is unitary and we get

$$\begin{aligned} L = (\mathfrak{o}y_1 + \mathfrak{o}y_2) \oplus (\mathfrak{o}\bar{x}_3 + \mathfrak{o}\bar{x}_4) \oplus J^* &= (\mathfrak{o}y_1 + \mathfrak{o}y_2) \oplus (\mathfrak{o}z_3 + \mathfrak{o}z_4) \oplus J^* \\ &= (\mathfrak{o}y_1 + \mathfrak{o}y_2) \oplus (\mathfrak{o}y_3 + \mathfrak{o}y_4) \oplus K. \end{aligned}$$

Now $(\mathfrak{o}x_1 + \mathfrak{o}x_2)$ and $(\mathfrak{o}z_3 + \mathfrak{o}z_4)$ both represent $[\pi^{u(1)}]$; so it suffices for us to prove that $(\mathfrak{o}x_1 + \mathfrak{o}x_2) \cong (\mathfrak{o}y_1 + \mathfrak{o}y_2) \bmod \mathfrak{b}_1$ and that $(\mathfrak{o}z_3 + \mathfrak{o}z_4) \cong (\mathfrak{o}y_3 + \mathfrak{o}y_4) \bmod \mathfrak{b}_1$. On grounds of symmetry, this reduces to the single problem of proving $(\mathfrak{o}x_1 + \mathfrak{o}x_2) \cong (\mathfrak{o}y_1 + \mathfrak{o}y_2) \bmod \mathfrak{b}_1$.

If $u(2)$ and $u(1)$ are of opposite parity, we have $x_1{}^2 \equiv y_1{}^2 \bmod \mathfrak{b}_1$, $x_2{}^2 \equiv y_2{}^2 \bmod \mathfrak{b}_1$, $x_1 \cdot x_2 \equiv y_1 \cdot y_2 \bmod \pi^{s(2)}$, and the result follows if we observe that $x_2{}^2(1 + \{\pi^{s(2)}\})^2 \equiv x_2{}^2 \bmod \mathfrak{b}_1$.

We now assume that $u(1) < u(2)$ have the same parity. In this case $X_1{}^2 = a^2 a_2 + \{\pi^{v(2)}\} \equiv a^2 a_2 \bmod \mathfrak{b}_1$; while $\epsilon\pi^{u(1)} \cong a_1 \bmod \pi^{v(1)}$ implies that $\epsilon\pi^{u(2)} \cong a_2 \bmod \mathfrak{b}_1$. Similarly with X_2. Hence we may take

$$X_1{}^2 \equiv a^2 \epsilon\pi^{u(2)} \bmod \mathfrak{b}_1, \qquad X_2{}^2 \equiv b^2 \epsilon\pi^{u(2)} \bmod \mathfrak{b}_1,$$

where a and b are integers. We therefore have

$$x_1{}^2 \equiv \epsilon\pi^{u(1)}(1 + a\pi^{\frac{1}{2}(u(2)-u(1))})^2 \bmod \mathfrak{b}_1.$$

Replace x_1 and x_2 by

$$(1 + a\pi^{\frac{1}{2}(u(2)-u(1))})^{-1} x_1 \text{ and } (1 + a\pi^{\frac{1}{2}(u(2)-u(1))})(x_1 \cdot x_2)^{-1} x_2$$

respectively. An easy computation shows that this second vector has norm

$\alpha\pi^{v(1)} - B^2\epsilon\pi^{u(2)} \bmod \mathfrak{b}_1$; so we have $(\mathfrak{o}x_1 + \mathfrak{o}x_2) \cong (\mathfrak{o}\omega_1 + \mathfrak{o}\omega_2) \bmod \mathfrak{b}_1$ where $\mathfrak{o}\omega_1 + \mathfrak{o}\omega_2$ has the matrix

$$\begin{pmatrix} \epsilon\pi^{u(1)} & 1 \\ 1 & \alpha\pi^{v(1)} - B^2\epsilon\pi^{u(2)} \end{pmatrix}, \qquad B \in \mathfrak{o}.$$

Now replace ω_2 by $(\omega_2 + B\pi^{\frac{1}{2}(u(2)-u(1))}\omega_1)\,(1 + \epsilon B\pi^{\frac{1}{2}(u(2)+u(1))})^{-1}$. Doing this we see that $(\mathfrak{o}x_1 + \mathfrak{o}x_2) \cong (\mathfrak{o}\omega_1 + \mathfrak{o}\omega_2) \cong (\mathfrak{o}y_1 + \mathfrak{o}y_2) \bmod \mathfrak{b}_1$. This proves the lemma.

PROPOSITION 8. *Let $L = \sum I_\lambda$ and $L = \sum M_\lambda$ be two canonical decompositions of L. If j is fixed $(1 \leqq j \leqq t)$, we can pass from $\sum I_\lambda$ to $\sum M_\lambda$ through a chain of canonical decompositions*

$$\sum I_\lambda \to \cdots \to \sum J_\lambda \to \sum K_\lambda \to \cdots \to \sum M_\lambda \tag{26}$$

such that under each transformation either (i) $\sum_1^j J_\lambda = \sum_1^j K_\lambda$ *or* (ii) $J_\lambda = K_\lambda\ (1 \leqq \lambda \leqq j-1)$.

Proof. We proceed by induction to $d = \dim(\sum_1^j I_\lambda)$. If $j = 1$ we are through. So assume that $j > 1$. We can take $s(1) = 0$. Let $\langle y\rangle$ denote a canonical basis corresponding to $\sum M_\lambda$.

Case 1. I_1 proper. Then we can write $y_1 = x_1 + X$ where $x_1 \in \sum_1^j I_\lambda$, $X \in \sum_{j+1}^t I_\lambda$. Since x_1^2 and y_1^2 are units, we can write $\sum_1^j I_\lambda$ in a canonical basis $\langle x\rangle$ having x_1 as its first element; this is the first transformation of the chain we are constructing and it satisfies the first condition of the proposition.

Apply $\mathrm{op}(x_1 \to x_1 + x_d)$ and put $X_1 = \mathrm{op}\, x_1$, $X_d = \mathrm{op}\, x_d$, $X_{d-1} = \mathrm{op}\, x_{d-1}$. Using (11) and (11a) it can be verified that $y_1 = \epsilon X_1 + \delta X_d + X$, where ϵ and δ are units. Put $X_d{}^* = X_d + \delta^{-1}X$ and express L in the semi-canonical basis

$$L = \mathfrak{o}X_1 \oplus (\mathfrak{o}x_2 + \cdots + \mathfrak{o}X_{d-1} + \mathfrak{o}X_d{}^*) \oplus (\mathfrak{o}z_{d+1} + \cdots + \mathfrak{o}z_n).$$

Apply $\mathrm{op}(X_1 \to X_1 + \epsilon^{-1}\delta X_d{}^*)$ and call the resulting basis $\langle z\rangle$. Then all the requirements of the proposition are satisfied by our chain of transformations. On the other hand $\epsilon z_1 = y_1$; we can apply the induction to the orthogonal complement of $\mathfrak{o}y_1$ to extend the chain from $\langle z\rangle$ to $\langle y\rangle$.

Case 2. I_1 improper. We can write $y_1 = x_1 + X$ with $x_1 \in \sum_1^j I_\lambda$, $X \in \sum_{j+1}^t I_\lambda$; since $y_1 \cdot y_2 = 1$, there must be a vector $x_2 \in \sum_1^j I_\lambda$ for which

$x_1 \cdot x_2 = 1$. Since $\mathfrak{o}x_1 + \mathfrak{o}x_2$ is unitary, we can suppose that x_1, x_2 is extended to a canonical basis for $\sum_1^t I_\lambda$. Apply $\operatorname{op}(x_1 \to x_1 + x_d)$ and put $X_1 = \operatorname{op} x_1$, $X_d = \operatorname{op} x_d$, $X_{d-1} = \operatorname{op} x_{d-1}$. Using (11) and (11b) it can be verified that $y_1 = \epsilon X_1 + \alpha x_2 + \delta X_d + X$, where ϵ and δ are units, $\alpha \in \mathfrak{o}$. Put $X_d{}^* = X_d + \delta^{-1} X$ and express L in the semi-canonical basis

$$L = (\mathfrak{o}(\epsilon X_1 + \alpha x_2) + \mathfrak{o}x_2) \oplus (\mathfrak{o}x_3 + \cdots + \mathfrak{o}X_{d-1} + \mathfrak{o}X_d{}^*)$$
$$\oplus (\mathfrak{o}z_{d+1} + \cdots + \mathfrak{o}z_n).$$

Now apply $\operatorname{op}(\epsilon X_1 + \alpha x_2 \to \epsilon X_1 + \alpha x_2 + \delta X_d{}^*)$ and call the resulting basis $\langle z \rangle$. Note that all these transformations are admissible in the sense that they satisfy the requirements of the proposition.

We now have $y_1 = z_1$, $y_2 = a_{12}z_1 + \cdots + a_{n2}z_n$; hence

$$y_1 \cdot (a_{12}z_1 + \cdots + a_{d2}z_d) = 1.$$

Replacing z_2 by $a_{12}z_1 + \cdots + a_{d2}z_d$, we see that we can assume that $y_2 = z_2 + Z$ with $Z \in \sum_{d+1}^n \mathfrak{o}z_\lambda$. We now proceed exactly as we did with y_1, and using admissible transformations only we arrive at a basis $\sum \mathfrak{o}z_\lambda{}'$ in which $(\mathfrak{o}y_1 + \mathfrak{o}y_2) = (\mathfrak{o}z_1{}' + \mathfrak{o}z_2{}')$. Then $\sum_3^n \mathfrak{o}z_\lambda{}' = \sum_3^n \mathfrak{o}y_\lambda$, and the induction completes the proof.

6. Unitary lattices modulo $\mathfrak{p}$. The Hasse symbol $S(L)$ of a given lattice L will play an important part in the rest of the paper. In the notation of Witt [WI], $S(L)$ is the product of quaternion algebras $\prod_{\lambda \leqq \mu} (a_\lambda, a_\mu)$ where $\sum a_\lambda{}^2 x_\lambda{}^2$ is any diagonal form associated with the metric in FL. When manipulating with these symbols we will use without further reference the rules of operation established on pp. 37-38 of Witt's paper [WI]. These results are valid over general fields; in addition, we have seen on p. 98 of [OI] that in a local field whose residue class field is perfect and of characteristic 2, the following relations are true:

$$(1 + 4\alpha, \epsilon) = 1, \tag{27}$$

$$(1 + 4\alpha, \epsilon\pi) = 1 \iff (1 + 4\alpha)^{\frac{1}{2}} \in F, \tag{28}$$

for any unit ϵ and any $\alpha \in \mathfrak{o}$.

Now let k be a rational integer, $0 < k \leqq e$. We contend that the quadratic form

$$(1 + \{4\pi^{1-k}\})x^2 + (1 + \{\pi^k\})y^2$$

represents 1. To this end we consider the lattice

$$L \cong (1 + \{4\pi^{1-k}\}) \oplus (1 + \{\pi^k\}).$$

It suffices to prove that L represents 1. Let us write L in the basis $\mathfrak{o}x_1 \oplus \mathfrak{o}x_2$ in which $L \cong (1 + [\pi^\gamma]) \oplus (1 + \{\pi^k\})$ with γ maximal. Then $|\pi^\gamma| \leqq |4\pi^{1-k}| \leqq |2\pi|$. Suppose if possible that $\gamma < \infty$. Then by Hensel's lemma, $\gamma \leqq 2e$; on the other hand, γ must be an odd number or we could apply $\mathrm{op}(x_1 \rightarrow x_1 + \alpha x_2)$ with α chosen so as to increase γ. Then there is a unit E such that

$$x_1^2 = 1 + E\pi^\gamma = (1 + \tfrac{1}{2}E\pi^\gamma)^2 - (\tfrac{1}{2}E\pi^\gamma)^2.$$

Hence we can in fact assume that $x_1^2 = 1 - (\tfrac{1}{2}E\pi^\gamma)^2$. Now apply $\mathrm{op}(x_1 \rightarrow x_1 + \tfrac{1}{2}E\pi^\gamma x_2)$; we see that $(x_1 + \tfrac{1}{2}E\pi^\gamma x_2)^2 = 1 + \{\pi^{2\gamma+k-2e}\}$ where $|\pi^{2\gamma+k-2e}| < |\pi^\gamma|$, and we have increased γ, which is impossible. Hence L represents 1. So the given quadratic form must represent 1. By putting $m = 2e + 1 - k$ we see that this result remains valid if $e < k \leqq 2e$. Hence we have

$$(29) \qquad ((1 + \{4\pi^{1-k}\}), \quad (1 + \{\pi^k\})) = 1 \qquad \text{if } 0 < k \leqq 2e.$$

We now prove that (A, B) can always be represented in the following way:

$$(30) \qquad (A, B) = (1 + 4C, \pi) \qquad \text{for some } C \in \mathfrak{o}.$$

First let A be a unit, B a prime; successive application of $\mathrm{op}(x_1 \rightarrow x_1 + \alpha x_2)$ to the lattice $L \cong Ax^2 + By^2$ shows that this form is equivalent to the form $(1 + \{4\})x^2 + D\pi y^2$; therefore we have $(A, B) = (1 + \{4\}, D\pi) = (1 + \{4\}, \pi)$ by (27). In general, we can suppose that A is either a unit or a prime; and similarly with B. If A and B are both units, then $(A, B) = (A, B\pi)(A, \pi) = (1 + \{4\}, \pi)$; if A and B are both primes, then

$$(A, B) = (B\pi^{-1}, A)(-A\pi^{-1}, \pi) = (1 + \{4\}, \pi). \qquad \text{q. e. d.}$$

In particular, (30) shows that the algebra classes (a, b) form a group over fields of our type. Now suppose that the Hasse symbols are not trivial over F. Then there is a unit ϵ such that $(1 + 4\epsilon)^{\frac{1}{2}} \notin F$; in other words, $x^2 + x - \epsilon$ is irreducible over F. Since this polynomial has distinct roots modulo π, it must be irreducible over the residue class field $\bar{F}$, by Hensel's lemma [AI]. Hence $\bar{F}$ has at least one quadratic extension. Conversely, let us assume that $\bar{F}$ has a quadratic extension and let $x^2 + \epsilon x + \delta$ be irreducible modulo π. Then $(1 - 4\delta\epsilon^{-2})^{\frac{1}{2}} \notin F$ and so the Hasse symbols are non-trivial over F.

THEOREM 1. *L and K are π^0-unitary lattices of the same dimension such that $v_L(1) = v = v_K(1)$ and $a_1(L) \cong a \cong a_1(K) \bmod \pi^v$ with $|a| \geqq |2|$. If $\mathfrak{p} \subseteq \pi^v\mathfrak{o}$, then $L \cong K \bmod \mathfrak{p}$ if and only if* (i) $d(L) \cong d \cong d(K) \bmod a\mathfrak{p}$, (ii) $(d(L), ad)S(L) = (d(K), ad)S(K)$ *when* $|\mathfrak{p}| < |4\pi^{-v}|$.

Proof. We write $|a| = |\pi^u|$.

Necessity. If we adjoin a hyperbolic plane to L and K, the resulting lattices are still isometric modulo $\mathfrak{p}$, and their u's and v's are the same as for L and K. It is easily seen that if (i) and (ii) are true for the enlarged lattices, then they are true for L and K. Hence we can assume that $\dim L = \dim K \geqq 3$. If L and K are proper, we can adjoin $J \cong (a)$ to L and K, and the same argument shows that we can assume that $\dim L = \dim K \geqq 4$ is an even number.

We have mentioned in (12)-(14) that a basis can be found for L in which $L = L_1 \oplus L_2 \oplus \sum H_\lambda$ where the H_λ are hyperbolic planes and

$$L_1 \cong \begin{pmatrix} b\pi^u & 1 \\ 1 & \{\pi^v\} \end{pmatrix}, \qquad L_2 \cong \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix}, \qquad |b| = 1.$$

Since $L \cong K \bmod \mathfrak{p}$ where $\mathfrak{p} \subseteq \pi^v\mathfrak{o}$, it follows from Lemma 2.2 in [OI] that we can obtain a decomposition $K_1 \oplus K_2 \oplus \sum M_\lambda$ for K in which

$$K_1 \cong L_1 \bmod \mathfrak{p}, \qquad K_2 \cong L_2 \bmod \mathfrak{p}, \qquad M_\lambda \cong H_\lambda \bmod \mathfrak{p}.$$

Calculating determinants in these bases proves that $d(L) \cong d(K) \pmod{\pi^u\mathfrak{p}}$, thereby proving the first result. We now define d as any unit satisfying the first relation. In order for (ii) to be non-vacuous, we assume that $\mathfrak{p} \subseteq (4\pi/\pi^v)\mathfrak{o}$. If $u = e$ we have $\mathfrak{p} \subseteq 2\pi\mathfrak{o}$, hence $L \cong K$ by Lemma 14.4 in [OI], and so (ii) holds. Hence we can suppose that $e > u$, $v > u$. Then it follows from the same result in [OI] that $L_2 \oplus \sum H_\lambda \cong K_2 \oplus \sum M_\lambda$.

We can write $K_1 \cong \begin{pmatrix} B\pi^u & 1 \\ 1 & \{\pi^v\} \end{pmatrix}$, where $B = b + \{4\pi/\pi^{u+v}\}$; we have $d_b \cong d_B + \{4\pi/\pi^{v-u}\}$ where $d_b = \det L_1$ and $d_B = \det K_1$. We know that $a\pi^{-u} \cong b \cong B (\bmod \pi^{v-u})$. An easy calculation with Hasse symbols gives

$$(d(L), ad)S(L)\,(d(K), ad)S(K) = (bB, -d_b)\,(d_b d_B, -a\pi^u B d d_b d(L)).$$

Using (29) it is easily verified that this expression is equal to 1. Hence we have $(d(L), ad)S(L) = (d(K), ad)S(K)$, and this proves the result.

Sufficiency. If L and K each contain a hyperbolic plane, then it is easily seen that (i) and (ii) are satisfied by the orthogonal complements

of these hyperbolic planes in L and K respectively. We can therefore assume that L and K do not both contain hyperbolic planes. In particular, we can assume that $1 < \dim L = \dim K \leqq 4$, since the proof of the 1-dimensional case is obvious, while any unitary lattice with dimension $\geqq 5$ must contain at least one hyperbolic plane. We can also suppose that $|\mathfrak{p}| < |\pi^v|$; for the case $\mathfrak{p} = \pi^v\mathfrak{o}$ follows immediately from (12)-(14).

Let us express L in a canonical basis. We can vary modulo $\mathfrak{p}$ a certain diagonal entry in the corresponding matrix for L to obtain a new lattice $L^* \cong L \bmod \mathfrak{p}$ for which $d(L^*) \cong d(K)$. It follows from the necessity of this theorem, already established, that L^* and K continue to satisfy the given conditions. In effect this means that we can take $d(L) \cong d(K)$ from the start.

Case 1. $|\mathfrak{p}| < |4\pi^{-v}|$. Since $d(L) \cong d(K)$, the second condition implies that $S(L) = S(K)$, and so L and K are field equivalent by Satz 17 in [WI]. In order to prove that $L \cong K$, we adjoin hyperbolic planes to L and K until we get two corresponding big lattices L' and K'. Then L' and K' are field equivalent, and they represent the same numbers by Proposition 5; hence $L' \cong K'$ by Theorem 19.1 of [OI]; hence $L \cong K$ by Proposition 3.

Case 2. $|\mathfrak{p}| \geqq |4\pi^{-v}|$. If $\dim L = 2$, since $|\pi^v| > |2|$ we can write

$$L \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \alpha\pi^v \end{pmatrix}, \qquad |\epsilon| = 1, |\alpha| = 1.$$

Then it is easy to see that K represents $\epsilon\pi^u \bmod 4\pi^{-v}$, hence $\bmod \mathfrak{p}$. We can therefore find a $K^* \cong K \bmod \mathfrak{p}$ such that K^* represents $\epsilon\pi^u$ and $d(L) \cong d(K^*)$. But such a K^* is isometric to L by Theorem 14.3 in [OI]. Hence $L \cong K \bmod \mathfrak{p}$.

If $\dim L = 3$, by (12)-(14) we can write

$$K \cong \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix} \oplus \epsilon, \qquad L \cong \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix} \oplus \delta$$

where ϵ and δ are units. The result is then immediate since $|\mathfrak{p}| \geqq |4\pi^{-v}|$ and since by a determinantal consideration $\epsilon \cong \delta \bmod \mathfrak{p}$.

Now consider the 4-dimensional case. u and v are of opposite parity since $|4\pi^{-v}| \leqq |\mathfrak{p}| < |\pi^v|$. We recall that we are taking $d(L) \cong d(K)$. By (30) we have $S(L)S(K) = (1 + 4E, \pi)$ for some $E \in \mathfrak{o}$. Write

$$K \cong \begin{pmatrix} \pi^v & 1 \\ 1 & 4\alpha\pi^{-v} \end{pmatrix} \oplus \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \beta\pi^r \end{pmatrix}$$

with ϵ a unit, α and β integral. Now consider

$$K^* \cong \begin{pmatrix} \pi^v & 1 \\ 1 & 4\alpha\pi^{-v} - 4E\pi^{-v} \end{pmatrix} \oplus \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \beta\pi^v - 4E\epsilon^{-1}\pi^{-u} \end{pmatrix}.$$

Clearly $K^* \cong K \bmod \mathfrak{p}$; and $d(L) \cong d(K^*) \cong d(K)$; computing Hasse symbols we get

$$S(K)S(K^*) = (\epsilon\pi^{u+v}, 1 + 4E) = (\pi, 1 + 4E),$$

using the fact that u and v have opposite parity. Hence $S(K^*) = S(L)$. Adjoining hyperbolic planes to L and K^* we get two lattices which are field equivalent and represent the same numbers; these lattices are isometric by Theorem 19.1 of [OI]; hence $L \cong K^*$; hence $L \cong K \bmod \mathfrak{p}$. This completes the proof of the theorem.

PROPOSITION 9. *L and K are unitary lattices and $\mathfrak{p}$ is an ideal in $\pi\mathfrak{o}$. If H and H' are unit hyperbolic planes and $H \oplus L \cong H' \oplus K \bmod \mathfrak{p}$, then $L \cong K \bmod \mathfrak{p}$.*

Proof. Suppose that $v = v_L \leqq v_K$. If $|\mathfrak{p}| \geqq |\pi^v|$, express L and K in the bases (12)-(14); then we easily see that $L \cong K \bmod \mathfrak{p}$. Now let $|\mathfrak{p}| < |\pi^v|$. Then all the lattices L, $H \oplus L$, $H' \oplus K$, K, have the same a's and v's. Apply the necessity of Theorem 1 to $H \oplus L$, $H' \oplus K$, then the sufficiency to L and K. q. e. d.

COROLLARY 9. *If L and K both represent the same number a of ordinal $u_L = u_K$, and if $H \cong \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \cong H'$, then*

$$H \oplus L \cong H' \oplus K \bmod \mathfrak{p} \Longrightarrow L \cong K \bmod \mathfrak{p}.$$

If a is a unit, the result holds for $H \cong (a) \cong H'$.

Proof. Let H have the basis $(\mathfrak{o}y_1 + \mathfrak{o}y_2)$ with $y_1^2 = a$, $y_2^2 = 0$. By the proposition we can assume that L and K are big. Hence we can write

$$L \cong \begin{pmatrix} -a & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \text{ in } (\mathfrak{o}x_1 + \mathfrak{o}x_2) \oplus \cdots.$$

Apply $\operatorname{op}(y_1 \to y_1 + x_1)$ and do the same with $H' \oplus K$. Now apply the proposition again. To prove the second half consider $a \oplus -a$ instead of the given H and H'. q. e. d.

7. The invariants. Now we can quickly derive our invariants. If $L = \sum L_\lambda$ is a canonical decomposition we define $\mathfrak{L}_j = L_1 \oplus L_2 + \cdots \oplus L_j$

for $1 \leqq j \leqq t$. The $\mathfrak{f}_\lambda$ are defined as in Section 5. The quantities $v(\lambda)$, a_λ, d_λ, appearing below are actually defined by the relations (i) and (ii), while the ideal $\mathfrak{d}_\lambda$ is the type invariant given by $d(\mathscr{L}_\lambda)\mathfrak{o} = \mathfrak{d}_\lambda = d(\mathscr{K}_\lambda)\mathfrak{o}$.

THEOREM 2. *Let L and K be two lattices of the same type and in the same space. Let $L = \sum L_\lambda$ and $K = \sum K_\lambda$ be canonical decompositions of L and K. Then L is isometric to K if and only if the following relations hold for all appropriate λ:*

(i) $$v_L(\lambda) = v(\lambda) = v_K(\lambda), \qquad a_\lambda(L) \cong a_\lambda \cong a_\lambda(K) \bmod \pi^{v(\lambda)},$$

(ii) $$d(\mathscr{L}_\lambda) \cong d_\lambda \cong d(\mathscr{K}_\lambda) \bmod \mathfrak{d}_\lambda \mathfrak{f}_\lambda,$$

(iii) $$|\pi^{v(\lambda+1)}\mathfrak{f}_\lambda| < |4\pi^{u(\lambda+1)}| \Longrightarrow (d(\mathscr{L}_\lambda), a_{\lambda+1}d_\lambda)\, S(\mathscr{L}_\lambda) = (d(\mathscr{K}_\lambda), a_{\lambda+1}d_\lambda) S(\mathscr{K}_\lambda),$$

(iv) $$|\pi^{v(\lambda)}\mathfrak{f}_\lambda| < |4\pi^{u(\lambda)}| \Longrightarrow (d(\mathscr{L}_\lambda), a_\lambda d_\lambda)\, S(\mathscr{L}_\lambda) = (d(\mathscr{K}_\lambda), a_\lambda d_\lambda) S(\mathscr{K}_\lambda).$$

Proof. If we adjoin a $\pi^{s(1)}$-hyperbolic plane to L we see that the *type* of L is unchanged and so it follows by inspection that the fundamental invariants a_λ, $v(\lambda)$, $\mathfrak{f}_\lambda$ are the same for the enlarged lattice as they are for L, $1 \leqq \lambda \leqq t$. In particular, if the same hyperbolic plane is adjoined to K it follows that the two new lattices will satisfy the relations (i)-(iv) if and only if L and K do. On the other hand, the enlarged lattices will be isometric if and only if $L \cong K$. Hence it suffices for us to consider big lattices only. Now suppose that $\dim L_j$ is an odd number for a certain j $(1 \leqq j \leqq t)$. Let us adjoin a lattice of type (a_j) to both L and K. Then the enlarged lattices will be isometric if and only if $L \cong K$, in virtue of the cancellation law established in Corollary 3. And it is easily verified that L and K have the same invariants (i)-(iv) if and only if the enlarged lattices do. Combining this with our first remark we see that we can assume that both L and K are big and that their components in any canonical decomposition are of even dimension. We shall assume that this is so.

Necessity. We can take $L = K$. The first result is then immediate. We now fix $j\,(1 \leqq j \leqq t)$ and we establish (ii) and (iv) for $\lambda = j$. A straightforward computation with the Hasse symbols shows that we can in fact take $s(j) = 0$. Construction: adjoin a lattice of type

$$\begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(j)} & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} a_{j+1} & \pi^{s(j+1)} \\ \pi^{s(j+1)} & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(j+1)} & \pi^{s(j+1)} \\ \pi^{s(j+1)} & 0 \end{pmatrix}$$

to L and call the resulting lattice L^*. Then the a_λ and $v(\lambda)$ are the same for L^* as for L, by (19). Hence this is also true for $\mathfrak{f}_\lambda$.

Now we can pass from $\sum L_\lambda$ to $\sum K_\lambda$ by a chain of transformations of the type described in Proposition 8. If we can establish (ii) and (iv) for each member of the chain, then we have established it for the given decompositions in virtue of the transitivity of the relations in question. Now (ii) and (iv) are obviously satisfied by a transformation of the first type since $\mathcal{L}_j$ and $\mathcal{K}_j$ do not change. It therefore suffices for us to prove the result for a transformation of the second type. In effect this allows us to assume that $L_\lambda = K_\lambda$ for $1 \leqq \lambda \leqq j-1$, and so

$$L_j^* \oplus L_{j+1}^* \oplus L_{j+2} \oplus \cdots \oplus L_t = K_j^* \oplus K_{j+1}^* \oplus K_{j+2} \oplus \cdots \oplus K_t.$$

Since the "$\mathfrak{f}_1$" for this lattice is precisely $\mathfrak{f}_j$, it follows from Lemma 1 that

$$(31) \qquad L_j^* \cong K_j^* \bmod \pi^{-u(j)}\mathfrak{f}_j, \qquad d(L_j^*)/d(K_j^*) \cong 1 \bmod \mathfrak{f}_j.$$

The second half of this result shows that $d(\mathcal{L}_j)/d(\mathcal{K}_j) \cong 1 \bmod \mathfrak{f}_j$, and so (ii) is established.

We now take d_j as defined by (ii) and we prove (iv). We assume that the condition $|\pi^{v(j)}\mathfrak{f}_j| < |4\pi^{u(j)}|$ is in fact satisfied for the j in question. Thus Theorem 1 when applied to (31) gives

$$(d(L_j^*), a_j d(L_j^*))S(L_j^*) = (d(K_j^*), a_j d(L_j^*))S(K_j^*)$$

and so $(d(L_j)d(K_j), a_j d(L_j))S(L_j)S(K_j) = 1$. Hence

$$(d(\mathcal{L}_j), a_j d_j)S(\mathcal{L}_j) \cdot (d(\mathcal{K}_j), a_j d_j)S(\mathcal{K}_j) = (d(L_j)d(K_j), d_j d(\mathcal{L}_j)).$$

and the right hand side of this equation is of the form

$$(1 + \{\mathfrak{f}_j\}, 1 + \{\mathfrak{f}_j\}) = (1 + \{2\}, 1 + \{2\pi\}),$$

which is equal to 1 by (29). This proves (iv).

We now prove (iii). Let $V(\lambda)$, A_λ, $\mathfrak{f}_\lambda^*$ denote the invariants under discussion when evaluated for $\mathfrak{R}L$. We have

$$V(t-\lambda+1) = v(\lambda) - 2s(\lambda), \qquad A_{t-\lambda+1} = a_\lambda \pi^{-2s(\lambda)}, \qquad \mathfrak{f}_{t-\lambda}^* = \mathfrak{f}_\lambda.$$

If we define $\mathcal{L}_\lambda^*$ as the sum of the first λ components in $\mathfrak{R}L = \mathfrak{R}L_t \oplus \cdots \oplus \mathfrak{R}L_1$, we see that $d(\mathcal{L}_\lambda^*) = \alpha^2 d(\mathcal{L}_{t-\lambda})d(L)$ where α is a certain field element. We put $d_\lambda^* = \alpha^2 d_{t-\lambda}d(L)$ and get

$$d(\mathcal{L}_\lambda^*) \cong d_\lambda^* \cong d(\mathcal{K}_\lambda^*) \quad \bmod d_\lambda^* \mathfrak{f}_\lambda^*.$$

Now suppose that condition (iii) is non-vacuous: then $|\pi^{v(j+1)}\mathfrak{f}_j| < |4\pi^{u(j+1)}|$.

Hence $|\pi^{V(t-j)}\mathfrak{f}_{t-j}^*| < |4\pi^{U(t-j)}|$. Apply condition (iv) (already proved) to $\Re L$ and we get

$$(d(\mathcal{L}_{t-j}^*), A_{t-j}d_{t-j}^*)S(\mathcal{L}_{t-j}^*) = (d(\mathcal{K}_{t-j}^*), A_{t-j}d_{t-j}^*)S(\mathcal{K}_{t-j}^*).$$

If we resubstitute in this equation, and use the fact that $d(\mathcal{L}_j)/d(\mathcal{K}_j) \cong 1 \bmod 2\pi$, we arrive at condition (iii). This completes the proof of the necessity.

Sufficiency. We are given that (i)-(iv) hold for the particular decompositions $\sum L_\lambda$, $\sum K_\lambda$. In virtue of the necessity (already proved) these conditions must hold for *any* two decompositions $L = \sum L_\lambda$, $K = \sum K_\lambda$. So we can assume that the given decompositions $\sum L_\lambda$, $\sum K_\lambda$ are supersaturated.

We shall prove the sufficiency by an induction on the *length* $s(t) - s(1)$ of L. That the induction can be made to start with lattices of zero length can be seen as follows: since L and K are big, condition (i) implies that they represent the same numbers, and so $L \cong K$ by Theorem 19.1 of [OI]. We note that (ii)-(iv) are vacuous for lattices of zero length. If we now proceed with the induction, it is easy to see that the given conditions are unaltered if we replace L and K by $\pi^k \circ L$ and $\pi^k \circ K$, and so we can take $s(1) = 0$. Since any unitary lattice of dimension $\geqq 5$ contains a hyperbolic plane, we can assume that $\dim L_1 = 4 = \dim K_1$. The basis of the inductive proof will be this: we must find decompositions $L = L_1' \oplus L'$, $K = K_1' \oplus K'$ with

$$L' = L_2' \oplus L_3 \oplus \cdots \oplus L_t, \qquad K' = K_2' \oplus K_3 \oplus \cdots \oplus K_t,$$

where $L_1' \cong K_1'$, and such that L_2', K_2' are still supersaturated components. Once such a reduction has been achieved, it is easy to see that L' and K' will also satisfy the conditions of the theorem. In point of fact, the quantities a_j, $v(j)$, $\mathfrak{f}_j$ are the same for L', K' as for L, K, only a simple relabelling being required. If d_j' is defined by $d_j' = d_j/d(L_1')$, the remaining conditions of the theorem must hold for L' and K'. For the rest of the proof call a saturated decomposition of the given L supersaturated if the first component represents a number of ordinal $v(1)$ while the remaining components are supersaturated. Similarly with the given K.

One further observation before we start the proof proper. If the supersaturated decompositions $\sum L_\lambda$, $\sum K_\lambda$ are such that $u(1)$ and $u(2)$ have the same parity and if $L_1 \cong K_1 \bmod \pi^{r(2)}$, then we can write $K_1 \oplus K_2$ in a new supersaturated decomposition

$$\bar{K}_1 \oplus \bar{K}_2 = K_1 \oplus K_2 \tag{32}$$

with $L_1 \cong K_1$. We prove this by writing L_1 and K_1 in the canonical bases $\mathfrak{o}x_1 + \mathfrak{o}x_2 + \mathfrak{o}x_3 + \mathfrak{o}x_4$ and $\mathfrak{o}y_1 + \mathfrak{o}y_2 + \mathfrak{o}y_3 + \mathfrak{o}y_4$ respectively, with $x_\lambda^2 = y_\lambda^2 + \alpha_\lambda$ where $\alpha_\lambda \in \pi^{v(2)}\mathfrak{o}$. Since K_2 represents α_λ, we can use Proposition 6 to express

$$K_2 \cong \begin{pmatrix} \alpha_\lambda & \pi^{s(2)} \\ \pi^{s(2)} & 0 \end{pmatrix} \oplus \cdots,$$

where the second component in the above isometry still represents the entire group $a_2\mathfrak{o}^2 + \pi^{v(2)}\mathfrak{o}$. Now apply $\mathrm{op}(y_\lambda \to y_\lambda + y_5)$ to get a new K_1 with $x_\lambda^2 = y_\lambda^2$. Doing this for $\lambda = 1, 2, 3, 4$ gives the desired result (32).

Case 1. $u(2) = u(1)$. The first component cannot therefore be proper. Consider $L = \sum L_\lambda$. Since L_2 represents $[\pi^{u(1)}]$, we can use Proposition 6 to apply successive changes of basis to L until we find a decomposition $L = L_1' \oplus L_2' \oplus L_3 \oplus \cdots \oplus L_t$ in which L_2' is still supersaturated, and such that

$$L_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(1)} & 1 \\ 1 & 4\alpha\pi^{-v(1)} \end{pmatrix},$$

where $\alpha = 0$ when $u(1)$ and $v(1)$ have the same parity or when $|\pi^{v(2)}| \geqq |4\pi^{-v(1)}|$. This construction uses the "op" transformations mentioned in (11) and is similar to the construction used in Lemma 16.3 of [OI]. We omit the details.

We repeat the construction on $K = \sum K_\lambda$. If $u(1)$ and $v(1)$ have the same parity, or if $|\pi^{v(2)}| \geqq |4\pi^{-v(1)}|$, then $L_1' \cong K_1'$ and so

$$L_2' \oplus L_3 \oplus \cdots \oplus L_t \cong K_2' \oplus K_3 \oplus \cdots \oplus K_t$$

by the inductive assumption. We can therefore assume that $u(1) + v(1)$ is odd, $|\pi^{v(2)}| < |4\pi^{-v(1)}|$,

$$(33) \quad L_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(1)} & 1 \\ 1 & 4\alpha\pi^{-v(1)} \end{pmatrix}, \quad K_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(1)} & 1 \\ 1 & 4\beta\pi^{-v(1)} \end{pmatrix}.$$

By (23) we have $\mathfrak{f}_1 = \pi^{u(1)+v(1)}\mathfrak{o}$. Then $|\pi^{v(2)}\mathfrak{f}_1| = |\pi^{v(2)+u(1)+v(1)}| < |4\pi^{u(1)}| = |4\pi^{u(2)}|$. Then (iii) must hold for these decompositions of L and K, i.e.

$$(d(L_1'), a_2d_1)S(L_1') = (d(K_1'), a_2d_1)S(K_1'),$$

and so $((1-4\alpha)(1-4\beta), a_2d_1\pi^{v(1)}) = 1$. Using (28) this implies that $(1-4\alpha) \cong (1-4\beta)$ and so $L_1' \cong K_1'$. Again we can apply the induction. This completes the first case.

Case 2. $u(2) = u(1) + 1$. Applying a little extra care when $u(1) = 0$, we can proceed as in Case 1 to get decompositions in which

$$(34)\qquad L_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} a_1 & 1 \\ 1 & 4\alpha\pi^{-u(1)} \end{pmatrix}, \quad K_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} a_1 & 1 \\ 1 & 4\beta\pi^{-u(1)} \end{pmatrix},$$

where $\alpha = \beta = 0$ when $|\pi^{v(2)}| \geqq |4\pi^{-u(1)}|$. So we consider $|\pi^{v(2)}| < |4\pi^{-u(1)}|$. Then $|\pi^{v(2)}\mathfrak{f}_1| = |\pi^{v(2)+u(1)+u(2)}| < |4\pi^{u(2)}|$. Condition (iii) again gives $L_1' \cong K_1'$. Thus Case 2 is established.

Case 3. $u(1) = e$. In virtue of Cases 1 and 2, we can assume that $|\pi^{u(2)}| \leqq |\pi^{u(1)+2}| = |2\pi^2|$. Then we easily see that $|\mathfrak{f}_1| \leqq |4\pi|$. Now

$$L_1 \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 2 & 1 \\ 1 & \{2\} \end{pmatrix}, \qquad K_1 \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 2 & 1 \\ 1 & \{2\} \end{pmatrix}.$$

But $d(L_1) \cong d(K_1) \bmod 4\pi$. Hence $L_1 \cong K_1$. So this case is proved.

Case 4. $s(2) = s(1) + 1$. Then in virtue of the first three cases we can take $u(1) < e$, $u(2) = u(1) + 2$. Also $s(1)$ is assumed to be 0, and so $s(2) = 1$. Then the behaviour of $v(1)$ and $v(2)$ can affect our result in three different ways. In the first place, we may have $|\pi^{v(1)}| > |2|$, and so $|\pi^{v(2)}| \geqq |\pi^{v(1)+2}|$. Then by (25) we have $\mathfrak{f}_1 = \pi^{v(2)+u(1)}\mathfrak{o}$, hence $d(L_1) \cong d(K_1) \bmod \pi^{v(2)+u(1)}$. But $|\pi^{v(2)}| \geqq |\pi^{v(1)+2}| \geqq |4\pi^{-v(1)}|$, since $|\pi^{v(1)}| > |2|$. Hence $L_1 \cong K_1 \bmod \pi^{v(2)}$ by Theorem 1. We can therefore write K in the supersaturated decomposition $K = K_1' \oplus K_2' \oplus K_3 \oplus \cdots \oplus K_t$ in which $L_1 \cong K_1'$. We then use the inductive hypothesis to arrive at the isometry $L \cong K$. In the second place, we may have $v(1) = e = v(2)$. Then obviously $L_1 \cong K_1 \bmod 2$. Hence we can find a supersaturated decomposition $K = K_1' \oplus K_2' \oplus K_3 \oplus \cdots \oplus K_t$ in which $K_1' \cong L_1$. Again we are through. Thirdly and finally, we may have $v(1) = e < v(2)$; then in fact $v(2) = e + 1$. Since $\mathfrak{f}_1 = 2\pi^{u(1)+1}\mathfrak{o}$, $\pi^{v(1)}\mathfrak{f}_1 = 4\pi \cdot \pi^{u(1)}\mathfrak{o}$, condition (iv) must be non-vacuous and we get

$$(d(L_1), a_1d_1)S(L_1) = (d(K_1), a_1d_1)S(K_1).$$

Thus $L_1 \cong K_1 \bmod 2\pi$ by Theorem 1. Hence the result follows from (32).

Case 5. $s(2) > s(1) + 1$. We can take $u(1) < e$, $u(2) \geqq u(1) + 2$. Define N_* as the orthogonal sum of six π^1-hyperbolic planes and let L^* and K^* be defined by the canonical decompositions

$$L^* = L_1 \oplus N_* \oplus L_2 \oplus \cdots \oplus L_t, \qquad K^* = K_1 \oplus N_* \oplus K_2 \oplus \cdots \oplus K_t.$$

Now it follows immediately from the definition of the quantities involved that $u^*(j) = u(j)$, $v^*(j) = v(j)$, $a_j^* = a_j$ for $j = 1, 2, 3, \cdots, t$. Hence

$$(35)\qquad \mathfrak{f}_j^* = \mathfrak{f}_j \qquad \text{for } j = 2, 3, 4, \cdots, t.$$

All these quantities are clearly the same for L^* as for K^*. We agree to

drop the *'s except for emphasis. Notice that the notation has suffered a minor inconsistency in passing from L to L^*. Thus a_1^* and $v^*(1)$ still refer to $L_{(0)}^*$. But for $j \geqq 2$ we are now using a_j^* and $v^*(j)$ to describe $L_{(s(j))}^*$, although strictly speaking they should be relabelled a_{j+1}^* and $v^*(j+1)$ with j running from 0 to t. Similar remarks apply to $\mathfrak{f}_j^*$. We shall use a_* and $v(*)$ to describe the numbers represented by $L_{(1)}^*$.

How are a_*, $v(*)$, $\mathfrak{f}_1^*$, and $\mathfrak{f}_*^* = \mathfrak{f}_*$ related? Since $u(*) = u(1) + 2$, we can take $a_* = a_1\pi^2$. We also have

$$v(1) \leqq v(*) \leqq v(1) + 2, \qquad v(*) \leqq e + 1.$$

Note that $L_{(1)}^*$ and $K_{(1)}^*$ represent the same numbers and so $v(*)$ is the same for both. If we choose a semi-canonical basis $\langle x \rangle$ corresponding to the supersaturated decomposition $\sum L_\lambda$ in which L_1 and L_2 both have the form (12)-(14), we easily see from (21) that

$$\mathfrak{f}_1^* \supseteq \mathfrak{f}_1, \qquad \mathfrak{f}_* \supseteq \mathfrak{f}_1. \tag{36}$$

Let us consider the invariants of L^* and K^*. We put $d_1^* = d_1$, $d_* = \pi^{12} d_1$, $d_\lambda^* = \pi^{12} d_\lambda$ for $2 \leqq \lambda \leqq t$. Then condition (i) holds between L^* and K^* for all λ. By (35) and (36) we see that for $\lambda = 1, *, 2, 3, \cdots, t$,

$$d(\mathcal{L}_\lambda^*) \cong d_\lambda^* \cong d(\mathcal{K}_\lambda^*) \bmod \mathfrak{f}_\lambda^* d_\lambda^*.$$

Now consider (iv) for the two enlarged lattices. If we have $|\pi^{v(1)}\mathfrak{f}_1^*| < |4\pi^{u(1)}|$, then $|\pi^{v(1)}\mathfrak{f}_1| < |4\pi^{u(1)}|$, in virtue of (36), and so (iv) holds when $\lambda = 1$. If $\lambda = *$, and $|\pi^{v(*)}\mathfrak{f}_*| < |4\pi^{u(*)}|$, then

$$|\pi^{v(1)}\mathfrak{f}_1| \leqq |\pi^{v(*)-2}\mathfrak{f}_*| < |4\pi^{u(*)-2}| = |4\pi^{u(1)}|;$$

hence

$$(d(\mathcal{L}_1), a_1 d_1) S(\mathcal{L}_1) = (d(\mathcal{K}_1), a_1 d_1) S(\mathcal{K}_1)$$

and so

$$(d(\mathcal{L}_*^*), a_* d_*) S(\mathcal{L}_*^*) = (d(\mathcal{K}_*^*), a_* d_*) S(\mathcal{K}_*^*).$$

Condition (iv) is immediate for $\lambda = 2, 3, \cdots, t$.

Now consider condition (iii). For $\lambda = 1$, we have $|\pi^{v(*)}\mathfrak{f}_1^*| = |\pi^{u(1)+2v(*)}| \geqq |4\pi^{u(*)}|$ since $|\pi^{v(*)}| \geqq |2\pi|$. Thus (iii) is vacuous when $\lambda = 1$. On the other hand it follows from (35) and (36) that (iii) holds when $\lambda = *, 2, 3, \cdots, t$.

We have therefore shown that L^* and K^* satisfy the invariants of the theorem. Now L^* and K^* have length $s(t) - s(1) = s(t)$; and the result has been established for lattices of this length which satisfy $s(2) = s(1) + 1$;

hence $L^* \cong K^*$; hence $L \cong K$ by Proposition 3. This completes the proof of Theorem 2.

Condition (ii) of Theorem 2 gives a determinantal description of how $\mathfrak{L}_j$ varies as we change the canonical decomposition $L = \sum L_\lambda$ of L. If we define

$$\mathfrak{b}_1 = \pi^{2s(1)-u(1)}\mathfrak{f}_1, \qquad \mathfrak{b}_j = \pi^{2s(j)-u(j)}(\mathfrak{f}_{j-1} + \mathfrak{f}_j), \qquad \mathfrak{b}_t = \pi^{2s(t)-u(t)}\mathfrak{f}_{t-1}.$$

we shall see that these quantities describe the change in the j-th component of $\sum L_\lambda$. Note that $\mathfrak{b}_j(\alpha \circ L) = \alpha\mathfrak{b}_j(L)$.

THEOREM 3. $\sum L_\lambda = L = \sum K_\lambda$ *are two saturated canonical decompositions of* L. *Then* $L_j \cong K_j \bmod \mathfrak{b}_j$ *for* $1 \leqq j \leqq t$.

Proof. In virtue of Proposition 9 we can assume that L is a big lattice. It suffices to prove the result when $s(j) = 0$ and when one of the decompositions, let us say $\sum L_\lambda$, is supersaturated. Let a_j be represented by K_j; then it is represented by L_j since $\sum L_\lambda$ is supersaturated. So we can assume that $\dim L_j$ is even, by Corollary 9. If $j = 1$ we have $L_1 \cong K_1 \bmod \mathfrak{b}_1$ by Lemma 1. If $j = t$ the result follows by considering $\mathcal{R}L$ instead of L.

Now suppose that $1 < j < t$. Adjoin

$$\begin{pmatrix} a_{j-1} & \pi^{s(j-1)} \\ \pi^{s(j-1)} & 0 \end{pmatrix} \oplus \begin{pmatrix} a_j & \pi^{s(j)} \\ \pi^{s(j)} & 0 \end{pmatrix} \oplus \begin{pmatrix} a_{j+1} & \pi^{s(j+1)} \\ \pi^{s(j+1)} & 0 \end{pmatrix}$$

to L and call the new lattice L^*. Then we can pass from $\sum L_\lambda^*$ to $\sum K_\lambda^*$ through a chain of transformations

$$\sum L_\lambda^* \to \cdot\ \cdot\ \cdot \to \sum I_\lambda^* \to \sum J_\lambda^* \to \cdot\ \cdot\ \cdot \to \sum K_\lambda^*$$

such that each I_λ^* represents $a_\lambda (j-1 \leqq \lambda \leqq j+1)$ and such that either $\sum_j^t I_\lambda^* = \sum_j^t J_\lambda^*$ or $\sum_1^j I_\lambda^* = \sum_1^j J_\lambda^*$. If the transformation is of the first type we have $I_j^* \cong J_j^* \bmod \mathfrak{b}_j$ by Lemma 1, since $\mathfrak{f}_1(\sum_j^t L_\lambda^*) \subseteq \mathfrak{f}_j \subseteq \pi^{u(j)}\mathfrak{b}_j$. If the transformation is of the second type we can deal with $\mathcal{R}L^*$ instead of L^* and we again get $I_j^* \cong J_j^* \bmod \mathfrak{b}_j$. Hence $L_j^* \cong K_j^* \bmod \mathfrak{b}_j$. Hence $L_j \cong K_j \bmod \mathfrak{b}_j$ by Corollary 9. q. e. d.

8. Concluding remarks. Our main result, Theorem 2, expresses the invariants of L in terms of the fundamental invariants a_j and $v(j)$ which were derived from the simplest invariant substructures of L. We now show that the numerical computation of these quantities can be reduced to the field problem of computing quadratic residues.

Since we can express L in a canonical basis using elementary operations only, we suppose that L is expressed in a semi-canonical basis $\sum \mathfrak{o} x_\lambda$. Write $t(\lambda) = \operatorname{ord} x_\lambda \cdot L$. Then $t(1) \leqq t(2) \leqq \cdots \leqq t(n)$. The basis $\langle x \rangle$ induces a canonical decomposition $L = \sum L_\lambda$ on L where the $s(j)$'s and $t(\lambda)$'s have the same range of values. Now we can easily define a_j: a_j is the greatest of the field elements

$$\pi^{2s(j)-2t(\lambda)} x_\lambda{}^2, \quad x_\gamma{}^2, \quad 2\pi^{s(j)}$$

under the given valuation, where x_λ runs through $L_1 \oplus \cdots \oplus L_{j-1}$ and x_γ runs through $L_j \oplus \cdots \oplus L_t$.

Suppose that all a_j have been determined. *Contention*:

$$\pi^{v(j)}\mathfrak{o} = \sum \pi^{2s(j)-2t(\lambda)} x_\lambda{}^2 \mathfrak{g}(a_j x_\lambda{}^2) + \sum x_\gamma{}^2 \mathfrak{g}(a_j x_\gamma{}^2) + 2\pi^{s(j)}\mathfrak{o}, \tag{37}$$

where x_λ runs through $L_1 \oplus \cdots \oplus L_{j-1}$ and x_γ runs through $L_j \oplus \cdots \oplus L_t$.

Proof of contention. We write $\pi^\mu \mathfrak{o}$ for the ideal defined in (37). We must prove that $\mu = v(j)$. We can take $s(j) = 0$. If we consider $\mathfrak{P}L$ we see that $\mu_L(j) = \mu_{\mathfrak{P}L}(1)$, while $v_L(j) = v_{\mathfrak{P}L}(1)$ by definition of $v(j)$. Thus we can assume that $j = 1$ and $s(1) = 0$. We must therefore prove that $v(1) = \mu$ where

$$\pi^\mu \mathfrak{o} = \sum x_\gamma{}^2 \mathfrak{g}(a_1 x_\gamma{}^2) + 2\mathfrak{o}.$$

First we prove $|\pi^{v(1)}| \geqq |\pi^\mu|$. This clearly holds if $\mu = e$; hence we assume that $\mu < e$, hence $\pi^\mu \mathfrak{o} = x_i{}^2 \mathfrak{g}(a_1 x_i{}^2)$ for some i. If $x_i{}^2 \in \pi^{v(1)}\mathfrak{o}$, we are through. Hence suppose that $x_i{}^2 = a_1 \alpha^2 + \{\pi^{v(1)}\}$ with $|a_1 \alpha^2| > |\pi^{v(1)}|$. Then

$$\pi^\mu \mathfrak{o} = \alpha^2 a_1 \mathfrak{g}(1 + \{\alpha^{-2} a_1{}^{-1} \pi^{v(1)}\}) \subseteq \pi^{v(1)}\mathfrak{o}.$$

Conversely we prove $|\pi^{v(1)}| \leqq |\pi^\mu|$. Suppose if possible that $|\pi^{v(1)}| > |\pi^\mu|$. So $|\pi^{v(1)}| > |2|$. Then we must have $x_\lambda{}^2 = \alpha_\lambda{}^2 a_1 + \beta_\lambda \pi^{v(1)+1}$ for all λ. Now any $x \in L$ can be written $\sum c_\lambda x_\lambda$. Then

$$x^2 \equiv \sum \alpha_\lambda{}^2 c_\lambda{}^2 a_1 \equiv (\sum \alpha_\lambda c_\lambda)^2 a_1 \bmod \pi^{v(1)+1}.$$

In particular, this is true for a vector x whose norm has ordinal $v(1)$. This is impossible since $v(1)$ and $u(1)$ have opposite parity when $|\pi^{v(1)}| > |2|$. q. e. d.

Let us call a big lattice L *dense* if $s(\lambda + 1) = s(\lambda) + 1$ for $1 \leqq \lambda \leqq t - 1$. Then in virtue of Proposition 3 the problem of this paper is equivalent to the problem of finding when two dense lattices L and K are equivalent. It is worth noting that the results can be simplified if we restrict ourselves to dense lattices only. Thus the u's will satisfy (22); the $\mathfrak{f}$'s are given by

(23)-(25); and Theorem 2 can be established without considering Case 5 in the proof of the sufficiency.

We conclude by giving a counter-example to show that both the conditions (iii) and (iv) are required in our characterization. Let F be the field $R_2(\pi)$ where R_2 is the 2-adic numbers and π is a root of $x^8-2=0$. For any $E \in \mathfrak{o}$ define L as the lattice with associated matrix

$$\begin{pmatrix}\pi & 1\\ 1 & 0\end{pmatrix} \oplus \begin{pmatrix}2 & 1\\ 1 & 2E\end{pmatrix} \oplus \begin{pmatrix}\pi^3 & \pi\\ \pi & 0\end{pmatrix} \oplus \begin{pmatrix}\pi^5 & \pi^2\\ \pi^2 & 0\end{pmatrix} \oplus \begin{pmatrix}2\pi^2 & \pi^2\\ \pi^2 & 2\pi^2 E\end{pmatrix}.$$

Let K be given by the same matrix, but with $E=0$. We can suppose that the E in L is a unit for which $(1-4E,\pi)\neq 1$. For both L and K we have

$$a_1=\pi,\quad a_2=\pi^3,\quad a_3=\pi^5,\quad v(1)=e,\quad v(2)=e+1,\quad v(3)=e+2$$

$$\mathfrak{f}_1=2\pi^2\mathfrak{o},\quad \mathfrak{f}_2=2\pi^3\mathfrak{o}.$$

We see that (i)-(ii) hold for L and K. Also (iii) is satisfied, being vacuous. But (iv) does not hold. Hence by the necessity of Theorem 2, L and K cannot be isometric.

UNIVERSITY OF OTAGO,
NEW ZEALAND.

REFERENCES.

[AI] E. Artin, "Algebraic numbers and algebraic functions I," *Princeton University, New York University*, 1950-1951.

[AsI] K. Asano, "Über Moduln und Elementarteilertheorie im Körper, in dem Arithmetik definiert ist," *Japanese Journal of Mathematics*, vol. 20 (1950), pp. 55-71.

[DI] W. H. Durfee, "Congruence of quadratic forms over valuation rings," *Duke Mathematical Journal*, vol. 11 (1944), pp. 687-697.

[EI] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Berlin (1952).

[JI] B. W. Jones, "A canonical quadratic form for the ring of 2-adic integers," *Duke Mathematical Journal*, vol. 11 (1944), pp. 715-727.

[JII] ———, "The arithmetic theory of quadratic forms," *Carus Monographs*, No. 10, Mathematical Association of America, 1950.

[OI] O. T. O'Meara, "Quadratic forms over local fields," *American Journal of Mathematics*, vol. 77 (1955), pp. 87-116.

[OII] ———, "Witt's theorem and the isometry of lattices," *Proceedings of the American Mathematical Society*, vol. 7 (1956), pp. 9-22.

[PI] G. Pall, "The arithmetical invariants of quadratic forms," *Bulletin of the American Mathematical Society*, vol. 51 (1945), pp. 185-197.

[WI] E. Witt, "Theorie der quadratischen Formen in beliebigen Körpern," *Journal für die reine und angewandte Mathematik*, vol. 176 (1937), pp. 31-44.

ON JACOBI BRACKETS.*

By PHILIP HARTMAN.

Hypothesis (H): Let $z = z(x)$ be a solution of the pair of partial differential equations

$$(1_F) \qquad F(x, p, z) = 0, \qquad\qquad (1_G) \qquad G(x, p, z) = 0,$$

where z, F, G are scalar functions of class C^1 of their arguments,

$$x = (x^1, \cdots, x^n), \qquad p = (p^1, \cdots, p^n),$$

and $p = \operatorname{grad} z$ in (1).

A standard theorem states that if (H) holds and if z is of class C^2 (instead of merely C^1), then z is a solution of the partial differential equation

$$(2) \qquad [F, G] = 0,$$

where $[F, G]$, the Jacobi bracket, is the function of (x, z, p) defined by

$$(3) \qquad [F, G] = \sum_{k=1}^{n} (F_k(G^k + p^k G_z) - G_k(F^k + p^k F_z))$$

in terms of $F_k = \partial F / \partial p^k$, $F^k = \partial F / \partial x^k$ and the corresponding partial derivatives of G.

If F and G are linear in the components of p, then the additional assumption that z is of class C^2 is not needed in this assertion; cf. the results on Poisson parenthesis in Ostrowski [1] and the references there to Gillis, E. Schmidt and Perron.

Professor Wintner has raised the question whether or not the additional assumption that z is of class C^2 can be omitted in the general (non-linear) case. In this note, his question will be answered in the affirmative if $n = 2$ and, under an additional condition, if $n > 2$. For example, if $n \geqq 2$ and if one of the functions F or G is linear in the components of p, then the answer is in the affirmative; in particular, there will result a new simple proof for the case that both F and G are linear in the components of p.

The results will be obtained as corollaries of the theorems of Pliś [2]

* Received May 23, 1956.

on the existence of characteristics on a solution of a partial differential equation. His theorems are applicable by virtue of the following remark:

(*) Assume hypothesis (H). Suppose that, on some t-interval, $(x,p,z) = (x(t),p(t),z(t))$ is a solution of the system of differential equations for characteristics

$$(4)\qquad x^{k\prime} = F_k(x,p,z), \qquad p^{k\prime} = -F^k(x,p,z) - p^k F_z(x,p,z), \qquad z' = \sum_{k=1}^{n} p^k F_k(x,p,z),$$

where $' = d/dt$, and that $z(t) = z(x(t)), p(t) = \operatorname{grad} z(x(t))$. Then the relation (2) holds for $(x,p,z) = (x(t),p(t),z(t))$.

In order to verify this, note that $G(x(t),p(t),z(t)) = 0$, since z is a solution of (1_G). Differentiation of this relation $G = 0$ with respect to t is permitted and gives $\sum(G^k x^{k\prime} + G_k p^{k\prime}) + G_z z' = 0$. In view of (3), the relation (2) for $(x,p,z) = (x(t),p(t),z(t))$ follows from (4).

(i) Assume hypothesis (H) and $n = 2$. Then (2) holds for $(x,p,z) = (x, \operatorname{grad} z(x), z(x))$.

For convenience, let (x,y) and (p,q) be used instead of the vector notation x and p. The relation (2) holds at a point (x,y,p,q,z) if $F_p = F_q = G_p = G_q = 0$. Suppose that, at some point, say

$$(x,y,p,q,z) = (0,0,p(0,0),q(0,0),z(0,0)),$$

one of these partial derivatives, say F_p, is not 0. Then, in some neighborhood of that point, the partial differential equation $F = 0$ can be written in the form

$$(5)\qquad p = f(x,y,z,q),$$

where f is of class C^1 in its arguments. Also, (4) is equivalent to the system

$$(6)\qquad y' = -f_q, \qquad z' = f - qf_q, \qquad q' = f_y + qf_z, \qquad p' = f_x + pf_z,$$

where $' = d/dx$. According to Pliś [2], there exist for small $|x|$ (continuously differentiable) functions $y = y(x)$, $z = z(x)$, $q = q(x)$ satisfying the first three equations in (6) and the conditions $y(0) = 0$, $z(x) = z(x,y(x))$, $q(x) = z_y(x,y(x))$. It follows from (5) that $p(x) = z_x(x,y(x))$ has a continuous derivative $p'(x)$ and that the last equation in (6) is a consequence of the first three and of (5). Thus (i) follows from (*).

(ii) Assume hypothesis (H) and $n > 2$. Then (2) holds for $(x, p, z) = (x, \operatorname{grad} z(x), z(x))$ if the initial value problem

$$dx^k/dt = F_k(x, \operatorname{grad} z(x), z(x)), \qquad x(0) = x_0 \tag{7}$$

has a unique (local) solution for every point $x = x_0$ with the property that at least one of the partial derivatives $F_k = \partial F/\partial p^k$, where $k = 1, \cdots, n$, is not 0 at $(x, p, z) = (x_0, \operatorname{grad} z(x_0), z(x_0))$.

This follows from the above arguments and from a theorem of Pliś [2] concerning existence of characteristics on C^1-solutions of equations (5), where x, p, z are scalars, $y = (y^1, \cdots, y^n)$ and $q = (q^1, \cdots, q^n)$, $q^k = \partial z/\partial y^k$.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES

[1] A. Ostrowski, "Sur un théorème fondamental de la théorie des équations linéaires aux dérivées partielles," *Commentarii Mathematici Helvetici*, vol. 15 (1942/43), pp. 217-221.

[2] A. Pliś, "Characteristics of non-linear partial differential equations," *Bulletin de l'Académie Polonaise des Sciences*, Cl. III, vol. 2 (1954), pp. 419-422.

ON THE FINITE FACTOR GROUPS OF ABELIAN GROUPS OF FINITE RATIONAL RANK.*

By Shreeram Abhyankar.

1. Introduction. In our recent paper we have given a proposition (Proposition 1 of Section 3 of [2]) to the effect that a finite factor group of a torsion free abelian group of rational rank one is necessarily cyclic. In the present paper we generalize this result to groups of finite rational rank, namely, we shall prove the following theorem.

Theorem. *Let A be a torsion free abelian group of finite rational rank n and let B be a proper subgroup of A of finite index. Then A/B is a direct sum of m cyclic groups with $m \leqq n$.*

From this theorem, in view of Satz 3 of Krull [4] and Theorem 1 of [5], we obtain the following corollary.

Corollary. *Let K be an n-dimensional algebraic function field over an algebraically closed ground field k of characteristic zero, and let K^* be a galois extension of K. Let v^* be a real zero-dimensional valuation of K^*/k and let v be the K-restriction of v^*. Then the splitting group of v^* over v is a direct sum of m cyclic groups with $m \leqq n$.*

Now let us refer to the discussion of the resolution problem sandwiched between Theorems 2A and 9A of Section 9 of our paper [2]. There we raised a valuation-ramification theortic objection to Theorem Z, which leads us to conclude that Theorem Z must be weakened at least to the point as to read: . . . every singularity of $f[V_r]$ is an s-fold normal crossing with $s \leqq r+1$. In view of Theorem 2 of [1]. the above corollary says that as far as valuation-ramification theory is concerned, this weakened form of Theorem Z is unobjectionable. This resolution theoretic implication accounts for our interest in the theorem of the present paper.

2. Proof of the theorem. The proof of the theorem will be preceded by two propositions. We shall use the following notations. By R and Z we shall denote respectively the additive groups of the rational numbers and the integers. For a positive integer n, we shall denote by $Z(n)$ a cyclic group of order n. For a prime number p, we shall denote by $Z(p^{\infty})$ the additive

* Received May 2, 1956.

group of those rational numbers whose denominators are powers of p. For abelian groups $G, G_1, G_2, \cdots, G_m$, we shall denote by $\bigoplus_{i=1}^{m} G_i$ and $\bigoplus_{m} G$ respectively the direct sum of $G_1, G_2, \cdots, G_m$, and the direct sum of m isomorphic copies of G. For well known properties of finite abelian groups which we shall use, we refer to Chapter 3 of [6].

PROPOSITION 1. *Let $G = \bigoplus_{n} Z(p^{\infty})$ where p is a given prime number. Let A be a subgroup of G and let B be a proper subgroup of A of finite index. Then $A/B = \bigoplus_{i=1}^{m} Z(p^{a_i})$ where the a_i are unique integers such that $1 \leqq a_1 \leqq a_2 \leqq \cdots \leqq a_m$ and $m \leqq n$.*

Proof. Let G^* (respectively A^*) be the subgroup of elements u in G (respectively in A/B) such that $pu = 0$. Then $G^* = \bigoplus_{n} Z(p)$. Since the order of every element of G is a power of p, the same is true for elements of A/B. Since A/B is finite, we have $A/B = \bigoplus_{i=1}^{m} Z(p^{a_i})$ where the a_i are unique integers such that $1 \leqq a_1 \leqq a_2 \leqq \cdots \leqq a_m$. This direct sum decomposition of A/B implies that $A^* = \bigoplus_{m} Z(p)$. Let f denote the canonical homomorphism of A onto A/B. Let $u_1, u_2, \cdots, u_m$ be a basis of A^* and fix v_i in A such that $f(v_i) = u_i$. Let A_1 be the subgroup of A generated by $v_1, v_2, \cdots, v_m$; let $B_1 = pA_1$, and let $A_1{}^*$ be the subgroup of elements u of A_1 such that $pu = 0$. Then $B_1 \subset (A_1 \cap B)$ and $[A_1 : B_1] \leqq p^m$; since $f(A_1) = A_1/(A_1 \cap B) = A^*$ we must have $[A_1 : B_1] = p^m$ and $B_1 = A_1 \cap B$. Since A_1 is of finite order which is a power of p and since $A_1/B_1 = A^* = \bigoplus_{m} Z(p)$ we conclude that $A_1 = \bigoplus_{i=1}^{m} Z(p^{b_i})$. Therefore $A_1{}^* = \bigoplus_{m} Z(p)$. Since $A_1{}^*$ is a subgroup of G^* we must have $m \leqq n$.

PROPOSITION 2. *Let $G = \bigoplus_{n} (R/Z)$. Let A be a subgroup of G and let B be a proper subgroup of B of finite index. Then $A/B = \bigoplus_{i=1}^{m} Z(q_i)$ with $m \leqq n$.*

Proof. As in the proof of Proposition 1 of [2], $R/Z = \bigoplus_{p \in P} Z(p^{\infty})$ where P is the set of all prime numbers. Hence $G = \bigoplus_{p \in P} Z_n(p^{\infty})$ where $Z_n(p^{\infty}) = \bigoplus_{n} Z(p^{\infty})$. It is clear that $Z_n(p^{\infty})$ is the subgroup of exactly those elements of G whose orders are powers of p. Let A_p and B_p denote the subgroups respectively of A and B consisting of all those elements whose orders are powers of p. By Theorem [1] of [3], we have that $A = \bigoplus_{p \in P} A_p$

and $B = \bigoplus_{p \in P} B_p$. Hence $A/B = \bigoplus_{p \in P} (A_p/B_p)$. By Proposition 1 we have that for a given prime number p either $A_p = B_p$ or

$$A_p/B_p = \bigoplus_{i=1}^{m_p} Z(p^{a_{pi}})$$

with $1 \leqq a_{p1} \leqq a_{p2} \leqq \cdots \leqq a_{pm_p}$ and $m_p \leqq n$. Since A/B is finite, we must have $A_p = B_p$ for all prime numbers p except for a finite number, say $p_1, p_2, \cdots . p_s$. Then

$$A/B = \bigoplus_{i=1}^{s} (A_{p_i}/B_{p_i}).$$

Let $m = \max(m_{p1}, m_{p2}, \cdots, m_{p_s})$ and set $a_{p_ij} = 0$ if $m \geqq j > m_{p_i}$. For $j = 1, 2, \cdots, m$, let

$$q_j = \prod_{i=1}^{s} p_i^{a_{p_ij}}.$$

Then $A/B = \bigoplus_{i=1}^{m} Z(q_i)$, with $m \leqq n$.

Proof of the theorem. Since B is a subgroup of A of finite index, B is also of rational rank n. Let $u_1, u_2, \cdots, u_n$ be a rational basis of B. Then $u_1, u_2, \cdots, u_n$ is a rational basis also of A. Let $G = \bigoplus_n R$. Then there is a unique isomorphism of A into G which maps u_i (for $i = 1, 2, \cdots, n$) onto the element of G all of whose components (in the given direct sum decomposition of G) except the i-th one are zero and whose i-th component in 1. We shall assume that by this isomorpphism A has been identified with a subgroup of G. Let Z_n be the subgroup of G generated by $u_1, u_2, \cdots, u_n$. Let $G^* = G/Z_n$, $A^* = A/Z_n$, and $B^* = B/Z_n$. Then B^* is a proper subgroup of A^*, A^* is a subgroup of G^*, $G^* = \bigoplus_n (R/Z)$, and A/B is isomorphic to A^*/B^*. Now the theorem follows from Proposition 2.

COLUMBIA UNIVERSITY.

REFERENCES.

[1] S. Abhyankar, "On the ramification of algebraic functions," *American Journal of Mathematics*, vol. 77 (1955), pp. 575-592.

[2] ———, "Simultaneous resolution for algebraic surfaces," *American Journal of Mathematics*, vol. 78 (1956), pp. 761-790.

[3] I. Kaplansky, *Infinite abelian groups*, Ann Arbor, 1954.

[4] W. Krull, "Galoische Theorie bewerteter Körper," Sitzungsberichte der Bayerischen Akademie der Wissenschaften, München (1930), pp. 225-238.

[5] S. MacClane and O. F. G. Schilling, "Zero-dimensional branches of rank one on algebraic varieties," *Annals of Mathematics*, vol. 40 (1939), pp. 507-520.

[6] A. Speiser, *Die Theorie der Gruppen*, New York, 1943.